WIRELESS STIG

BLACKBERRY SECURITY CHECKLIST

Version 5, Release 2.1

15 November 2007

Developed by DISA for the DoD

Database Reference Number: ___________________

Database entered by: _____________________Date:_______

Technical Q/A by: _______________________Date:_______

Final Q/A by: ___________________________Date:_______

CAT I: _____

CAT II: _____

CAT III: _____

CAT IV: _____

TOTAL: _____

UNCLASSIFIED

Unclassified UNTIL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist
Confidential System = CONFIDENTIAL Checklist
Secret System = SECRET Checklist
Top Secret System = SECRET Checklist

Site Name:______________________________________ Date of Wireless SRR:______________________

Wireless Reviewer			**Phone/Location**		
Previous SRR (circle)	Y N	**Date of Previous SRR**			
Number of Current Open Findings					
Site Name					
Address					
Phone					

Position	**Name**	**Phone Number**	**Email**	**Area of Responsibility**
IAM				
IAO				
BlackBerry Administrator				

This page is intentionally blank.

TABLE OF CONTENTS

TABLE OF TABLES

Page

TABLE OF FIGURES

Page

This page is intentionally blank.

SUMMARY OF CHANGES

GENERAL CHANGES:

- The previous release was Version 5, Release 1.1, dated 20 February 2007

SECTION CHANGES

SECTION 1. INTRODUCTION

- Minor editorial changes.

SECTION 2. BLACKBERRY COMPLIANCE REQUIREMENTS

- Minor editing was performed on each check.
- Added more instructions on how each check should be reviewed during an SRR.
- Requirement WIR1130 has been updated to clarify the requirement.
- Changed WIR0360 to WIR0180 to be consistent with the Wireless Checklist.
- Changed WIR1030 to WIR0225 to be consistent with the Wireless Checklist.
- Changed WIR0560 to WIR 0011 to be consistent with the Wireless Checklist.
- Changed WIR0076 and added WIR0012 to comply with DoD CIO memorandum "Policy on Use of Department of Defense (DoD) Information Systems Standard Consent Banner and User Agreement," dated 2 Nov 2007 that requires specific information be included in user agreements.
- WIR0072, was added. This check was inadvertently deleted from the previous version of this document.
- WIR1015 was added to clarify the requirement for BlackBerry disposal.
- WIR1230 was deleted. Requirement has been included in WIR1170 to clarify BlackBerry activation requirements.
- WIR1150 was updated due to approval for using the Blackberry smart card reader with PCs.

SECTION 3. BES SECURITY RELATED CONFIGURATIONS

- Updated the following section: 3.8.
- Deleted 3.3.1 Installing NTLM on the BES. NTLM authentication is not authorized to DoD network web servers (DoD requires NTLMv2, which is not supported by the BES).
- Deleted 3.3.2 Access Control – Push and Pull Configuration
- Deleted 3.3.5 Configuring SSL
- Added new section, 3.3.1 Configuring BlackBerry Authentication To Web Servers
- Section 3.4, added new information on a recommended BES configuration change related to S/MIME.
- Added new section, 3.15 BlackBerry IP Modem
- Added new section, 3.16 Disposal of BlackBerry handhelds
- Added new section, 3.17 Use of Team or group BlackBerrys
- Added new section, 3.18 RIM Bluetooth Smart Card Reader Connections to PCs

APPENDIX A. REFERENCES

- Updated to remove outdated references and added new references.

APPENDIX B. BLACKBERRY DISPOSAL PROCEDURES

– New appendix. Appendix B in previous edition (BlackBerry Device Wiping and Nuking Procedures) has been deleted.

APPENDIX C. BES IT POLICY RULES

– Added columns with requirement numbers for all required IT Policy rule settings and a column for security reviewers to use to mark an open check.
– Minor changes to a number of Bluetooth Smart Card Reader group IT Policy rules.
– Added clarification information on several IT Policy rules for required configuration settings.
– Added new IT Policy rules released in version 4.1.3 of the BES.
– Several IT Policy rules that were previously "Required" and are now "Optional:"

- Disable BlackBerry Messenger
- Disable Notes Native Encryption Forward And Reply
- Show Web Link
- Force Memory Clean When Holstered
- Force Memory Clean When Idle
- Memory Cleaner Maximum Idle
- Download URL Images
- Download Themes URL
- Download Tunes URL
- Allow Outgoing Call When Locked
- Disable Key Store Backup
- Disable radio When Cradled
- Allow Other Message Services

– Please note new requirement for "Lock Owner Info" and Set Owner Info."

APPENDIX D. HANDHELD SOFTWARE CONFIGURATION SETTINGS

– Added columns with requirement numbers for all required IT Policy rule settings and a column for security reviewers to use to mark an open check.

APPENDIX E. CAC DIGITAL CERTIFICATE PROVISIONING

– This is a new Appendix.

APPENDIX F. VMS PROCEDURES

– Previously Appendix E.

APPENDIX G. BLACKBERRY CONFIGURATION FOR GROUP EMAIL ACCOUNTS

– This is a new Appendix.

1. INTRODUCTION

This *BlackBerry Security Checklist* when used with the *Wireless Security Technical Implementation Guide* (STIG) assists in the secure configuration and use of BlackBerry wireless email in the Department of Defense (DoD). Guidance in this document applies to all BlackBerry systems, including BlackBerry handheld devices and the BlackBerry Enterprise Server (BES).

This checklist serves as both a security review checklist and a configuration guide. Information Assurance Officers (IAOs), Security Managers (SMs), System Administrators (SAs), device users, and security readiness reviewers, each with varying experience levels, will use this document to ensure the security of BlackBerry implementations. Thus, the format of each section is tailored to meet these various needs.

Section 2 must be used by IAOs, SMs, and SAs for performing self-assessments. This section is also used by DISA FSO to perform Security Readiness Reviews (SRRs). Appendix F provides procedures used by SAs and SRR reviewers when registering and updating assets in the Vulnerability Management System (VMS).

Section 3 and Appendices B, C, D, E, and G are intended for experienced BES administrators who have completed BES 4.0/4.1 for Microsoft Exchange Administrator training. SAs should also consult Appendix A for a listing of various Research in Motion (RIM) configuration guides and other documents. The configuration settings (or actions) in Section 3 and Appendices C and D are classified as either “Required” or “Optional”. “Required” configuration settings are mandatory for all installations of DoD BES for Microsoft Exchange and for BlackBerry Handheld Software. “Optional” settings are the recommended and preferred configuration for installations of DoD BES 4.0/4.1 for Microsoft Exchange and BlackBerry Handheld Software. “Optional” configuration settings may not be possible at all DoD installations because of operational or network constraints.

This checklist covers configuration requirements for BES versions 4.0 to 4.1 (SP4) and BlackBerry Handheld Software version 4.0 to 4.2 Earlier versions of software are not authorized for use in DoD.

This checklist has the minimum “baseline” BlackBerry security guidance for DoD. Combatant Commanders/Services/Agencies (CC/S/A) may direct more secure configuration settings based on operational requirements.

For our NATO customers using this document:

> The term “classified” used in this document refers to US Government classifications of Confidential, Secret and Top Secret. NATO BlackBerry deployments are permitted to carry information bearing a NATO classification of “NATO restricted” and should be treated in a similar manner as US Government information marked Unclassified//For Official Use Only. The security guidance provided in this document can be directly applied to NATO BlackBerry deployments with the understanding that “NATO Restricted” information should not be equated to US Government-defined “classified” information.

This page is intentionally blank.

2. BLACKBERRY COMPLIANCE REQUIREMENTS

2.1 Classified Information

WIR0180 Wireless PEDs allowed into SCIFs must be DCID compliant.

CAT I	WIR0180	V0012072	MAC: 1, 2, 3	CL: C, S	IAC: ECWN-1	Ref: DCID 6/9 and 6/3

Vulnerability: PEDs are allowed in a SCIF without DCID compliance

The IAO will ensure wireless PEDs (e.g. wireless two-way email devices such as the BlackBerry) are not permitted in a SCIF unless approved in accordance with DCID 6/9 or 6/3 requirements.

Check: Work with the traditional reviewer or interview the IAO or SM.

1. Determine if site SCIF security policy/procedures allow users to bring PEDs into SCIFs.

– If No, determine if procedures are in place to prevent users from bringing PEDs into SCIFs and users are trained on this requirement. Posted signs are also evidence of compliance.

2. If Yes,

– Determine if site has written procedures that describe what type of PEDs and under what type of conditions (e.g. turned off, SCIF mode enabled)

– If PED devices are allowed, then users should receive proper training on the handling of these devices in a SCIF.

4. Mark this as a finding if:

– Required procedures or training policies are not in place or

– Required user training has not been documented.

Comments:

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0225 Use proper separation when using wireless PEDs around classified areas.

CAT II	WIR0225	V0012106	MAC: 1, 2, 3	CL: C	IAC: ECWN-1	Ref: DoDD 8100.2

Vulnerability: Wireless PEDs are used in classified areas.

The IAO will ensure wireless PEDs are not permitted or used in areas where classified data processing takes place unless:

- The DAA, in consultation with the CTTA, has approved the wireless PED for entry and/or use in the facility.

- The wireless PED is separated from the classified data equipment a distance determined by the CTTA and appropriate countermeasures, as determined by the CTTA, are implemented.

Check:
Review documentation. Work with the traditional security reviewer to verify the following.

1. If classified information is not processed at this site, or site has a written procedure prohibiting the use of wireless devices in areas where classified data processing occurs, then mark as not a finding.
2. Ask for documentation showing the CTTA was consulted about operation and placement of wireless devices. Acceptable proof would be coordination signature or initials of the CTTA on the architecture diagram or other evidence of coordination. IAW DoD policy, the CTTA must have a written separation policy for each classified area.
3. Review written policies, training material, or user agreements to see if wireless usage in these areas is addressed.
4. Verify proper procedures for wireless device use in classified areas is addressed in training program.
5. Mark as a finding if any of the following is found.

- CTTA has not designated a separation distance in writing
    - DAA has not coordinated with the CTTA
    - Users are not trained or made aware (using signage or user agreement) of procedures wireless device usage in and around classified processing areas.

Comments:

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0372 Do not allow PEDs with cameras into classified processing areas.

CAT I	WIR0372	V0012165	MAC: 1, 2, 3	CL: S, P	IAC: DCHW-1	Ref: DoDD 8100.2

Vulnerability: Wireless phones with cameras are allowed into classified areas.

The IAO will ensure PEDs with digital cameras (still and video) are not allowed in any SCIF or other area where classified documents or information is stored, transmitted, or processed.

Check: Interview the IAO and confirm compliance by reviewing site's physical security policy. The traditional reviewer may also assist in determining compliance.

1. Review site's physical security policy.
2. Verify that users are informed of this policy by reviewing user agreement, posted signs, or training material.
3. Powering off, removal of batteries or blocking IR ports is not acceptable for disabling camera functionality, as this method has not been tested for efficacy.
4. Mark as a finding if a written policy and user training does not prohibit these devices in classified areas.

Comments:

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR1010 Establish CMI procedures for wireless email devices and systems.

CAT II	WIR1010	V0011820	MAC: 1, 2, 3	CL: C, S	IAC: PRTN-1, VIIR-1, VIIR-2	Ref: DoDD 8530.2

Vulnerability: Wireless email device classified incident handling is not compliant.

The IAO will ensure that if a Classified Message Incident (CMI) occurs on a wireless email device or system, the following actions are completed.

For BlackBerry system:

In accordance with DoD policy, all components must establish Incident Handling and Response procedures. A Classified Message Incident (CMI) or "data spill" occurs when a classified email is inadvertently sent on an unclassified network and received on a BlackBerry device. BlackBerry systems are not authorized for processing classified data.

- The BlackBerry Enterprise Server (BES) and Microsoft Exchange server are handled as classified systems until they are sanitized according to appropriate procedures.

- The BlackBerry handheld is handled as a classified device and must be destroyed according to DoD guidance for destroying classified equipment. Currently, there is no reliable method for sanitizing BlackBerry handhelds after a CMI.

Check: Interview the IAO. Verify classified incident handling, response, and reporting procedures are documented and BlackBerry users are trained (or requirement listed on signed user agreement) on these requirements.

Comments:

Open	□	Not a Finding	□	Not Reviewed	□	Not Applicable	□

WIR1020 Do not use wireless email for classified messages.

CAT I	WIR1020	V0014016	MAC: 1, 2, 3	CL: C	IAC: ECWN-1	Ref: DoDD 8100.2

Vulnerability: Wireless email devices are used for classified.

The IAO will ensure wireless two-way email devices and systems are not used to send, receive, store, or process classified messages.

Check: Interview the IAO. Verify local written policy and user training (or requirement listed on signed user agreement) on this requirement.

Mark as a finding if users are not informed of this policy through training, user agreement, or posted signs.

Comments:

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR1040 Do not connect wireless email devices to classified computers.

CAT I	WIR1040	V0011832	MAC: 1, 2, 3	CL: C	IAC: ECWN-1	Ref: DoDD 8100.2

Vulnerability: Wireless email devices are connected to a classified network.

The IAO will ensure that BlackBerry devices and systems are not connected to classified DoD networks or information systems.

Check:
If possible, work with the traditional reviewer to determine compliance.

For BlackBerry System:
Verify written policy and training material exists (or requirement listed on signed user agreement) that states that either wireless devices or specifically BlackBerry devices must not be connected directly or indirectly (synched) to classified computers or networks.

Comments:

Open		Not a Finding		Not Reviewed		Not Applicable	

2.2 Unclassified Information

WIR0010 All Wireless systems must have DAA approval..

CAT I	WIR0010	V0008283	MAC: 1, 2, 3	CL: S, P	IAC: ECWN-1	Ref: DoDD 8100.2

Vulnerability: Use of unauthorized wireless devices and software.

The IAO will ensure all wireless systems (including associated peripheral devices, operating system, applications, network/PC connection methods, and services) are approved by the DAA prior to installation and use for processing DoD information.

Check: Work with the site POC to verify documentation. Performed with WIR0016 (equipment list).

1. Request copies of written DAA approval documentation

– A signed wireless inventory list, SSAA, or DAA approval documents as proof of compliance.

– DAA approval letter and SSAA may be a general statement of approval rather than list each device.

2. If site does not have a complete list of wireless equipment, the reviewer may use the *SRR Worksheets* in the *Wireless Security Checklist, Appendix B SRR Worksheets* to interview the SA and record equipment details.
3. Verify DAA approval for each device used (i.e., wireless connection services, peripherals, and applications).

Mark this check as a finding for any of the following reasons.

- Wireless systems, devices, services, or accessories are in use but DAA approval letter (s) do not exist
- If in the judgment of the reviewer, configuration differs significantly from that approved by the DAA approval letter.

Comments:

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0011 Personally owned PEDs need DAA approval and forfeiture agreement .

CAT III	WIR0011	V0014025	MAC: 1, 2, 3	CL: S, P	IAC: ECSC-1	Ref: Wireless STIG

Vulnerability: Personally owned devices are used**.**

The IAO will ensure personally owned PEDs are not used to transmit, receive, store, or process DoD information unless approved by the DAA and the owner signs forfeiture agreement in case of a security incident.

Check: Interview the IAO.

1. Ask if users are using personally owned devices such as PDAs, Blackberries, laptops, or home computers to access sensitive Enclave resources. Access to publicly available resources in the DMZ can be accessed via personal devices, depending on the INFOCON level.
2. If personally owned devices are allowed, verify written DAA approval exists and the SSAA is annotated.
3. Verify remote user agreement (including **forfeiture agreement**) or training material is used to train users on security this requirement.
4. Mark as a finding if:

- CAT I finding if personally owned devices are used for classified access.
- CAT III finding if forfeiture agreement or training is not part of site’s procedure or if users are allowed to use personally owned PEDs without DAA approval.

Hint: This check includes any non-DoD owned or approved devices such as computers, PEDs/PDAs, and wireless NICs. This applies to administrative and end-user access. Use for end-user is discouraged but may be approved by DAA.

Comments:

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0012 Display required DoD logon banner on PDA.

CAT III	WIR0016	V00015399	MAC: 1, 2, 3	CL: S, P	IAC: EBCR-1	Ref: DoD CIO Memo, 2 Nov 2007

Vulnerability: DoD Logon Banner not displayed.

The IAO will ensure all PDAs display the following banner during device unlock/ logon: “I've read & consent to terms in IS user agreement.”

Check:
For BlackBerry system
Work with the SA to review the configuration of the BES IT Policy rules. Reviewed as part of WIR1250 check.

Comments:

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0016 Maintain an equipment list of all approved wireless devices.

CAT III	WIR0016	V0008284	MAC: 1, 2, 3	CL: S, P	IAC: DCHW-1	Ref: DoDD 8100.2
Vulnerability: Wireless equipment list not available/updated						
The IAO will maintain a list of all DAA approved wireless devices. The list is stored in a secure location. **Check**: 1. Verify existence of site wireless equipment list. 2. Determine the process for updating the list and keeping it current. The list should indicate date of last update.						
Comments:						

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0030 Document equipment in the SSP

CAT III	WIR0030	V0008297	MAC: 1, 2, 3	CL: S, P	IAC: EBCR-1	Ref: Wireless STIG
Vulnerability: SSAA is not established or properly updated.						
The IAO will ensure wireless devices, which connect directly or indirectly (e.g., hot-sync, ActiveSync, wireless) to the network, are added to the SSP. **Check**: Review the SSP. 1. Wireless network devices such as access points, laptops, PEDs, and wireless peripherals (keyboards, pointers, etc.) that use a wireless network protocol such as Bluetooth, 802.11, or proprietary protocols must be documented in the SSP. 2. A general statement in the SSP permitting the various types of wireless network devices used by the site is acceptable rather than a by-model listing (e.g., a statement that “wireless devices of various models are permitted but only when configured in accordance with the Wireless STIG or other such specified restriction”). 3. Mark as a finding if a DAA approved SSP does not exist or if it is not updated.						
Comments:						

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0072 Wireless network devices must be physically protected.

CAT II	WIR0072	V0014894	MAC: 1, 2, 3	CL: C, S	IAC: PEPF-1, PEPF-2	Ref: DoDI 8500.2 NSA SECNET 11 CONOPS

Vulnerability: Communications devices not physically secured

The NSO will ensure all network devices (i.e., Intrusion Detection System (IDS), routers, servers, Remote Access System (RAS), firewalls, WLAN access points, etc) are located in a secure room with limited access or otherwise secured to prevent tampering or theft.

Check: Work with the traditional reviewer to verify.

1. During SRR walkthrough inspection, visually confirm that wireless APs, VoIP, IDS, and other network components are installed in secured areas.
2. Mark as a finding if wireless network hardware is not physically secured as required.

Comments:

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0076 Require signed user agreement.

CAT II	WIR0076	V0014020	MAC: 1, 2, 3	CL: S	IAC: PRTN-1	Ref: Wireless STIG
Vulnerability: User agreement is not compliant						

For mobile and remote users of the DoD enclave and resources, the IAM will develop a written security policy or checklist for secure wireless remote access to the site and an agreement between the site and remote user. These documents will include relevant security requirements, including (but not limited to) the following.

- The agreement will contain the type of access required by the user (privileged, end-user, etc.).
- The agreement will contain the responsibilities, liabilities, and security measures (e.g., malicious code detection training) involved in the use of the wireless remote access device.
- Incident handling and reporting procedures will be identified along with a designated point of contact.
- The remote user can be held responsible for damage caused to a Government system or data through negligence or a willful act.
- The policy will contain general security requirements and practices and are acknowledged and signed by the remote user.
- If classified devices are used for remote access from an alternative work site, the remote user will adhere to DoD policy in regard to facility clearances, protection, storage, distributing, etc.
- Government owned hardware and software is used for official duties only. The employee is the only individual authorized to use this equipment.

DoD CIO Memorandum “Policy on Use of Department of Defense (DoD) Information Systems Standard Consent Banner and User Agreement,” dated 2 Nov 2007 requires the following additional information in all User Agreements:

STANDARD MANDATORY NOTICE AND CONSENT PROVISION FOR ALL DOD INFORMATION SYSTEM USER AGREEMENTS
By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

- You are accessing a U.S. Government information system (as defined in CNSSI 4009) that is provided for U.S. Government-authorized use only.

- You consent to the following conditions:
  - The government routinely monitors communications occurring on this information system, and any device attached to this information system, for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network defense, quality control, employee misconduct investigations, law enforcement investigations, and counterintelligence investigations.
  - At any time, the government may inspect and/or seize data stored on this information system and any device attached *to* this information system.
  - Communications occurring on or data stored on this information system, or any device attached to this information system, are not private. They are subject to routine monitoring and search.
  - Any communications occurring on or data stored on this information system, or any device attached to this information system, may be disclosed or used for any U.S. Government-authorized purpose.
  - Security protections may be utilized on this information system to protect certain interests that are important to the government. For example, passwords, access cards, encryption or biometric access controls provide security for the benefit of the government. These protections are not provided for your benefit or privacy and may be modified or eliminated at the government's discretion.

Check:

1. Inspect a copy of the site’s user agreement.
2. Verify user agreement has the minimum elements described in the STIG policy.
3. The site’s training program may also be used for this purpose. Inspect a copy of the training materials.
4. User agreements and education is particularly important for mobile and remote users since there is a high risk of loss, theft, or compromise thus this signed agreement is a good best practice to help ensure the site is making the user is aware of the risks and proper procedures.
5. Mark as a finding if user agreement does not exist or is not compliant with the minimum requirements.

Comments:

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR0371 PEDs with cameras must be approved by physical security policies.

CAT III	WIR0371	V0004840	MAC: 1, 2, 3	CL: S, P	IAC: ECWN-1	Ref: DoDD 8100.2

Vulnerability: PED camera policy does not exist

The IAO will ensure PEDs with digital cameras (still and video) are allowed in a DoD facility only if specifically approved by site physical security policies.

Check: Review site’s physical security policy. Verify that it addresses PED devises with embedded cameras.

Mark this as a finding if there is no written physical security policy outlining whether wireless phones with cameras are permitted or prohibited on or in this DoD facility.

Comments:

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR1015 Establish disposal procedures for wireless email devices.

CAT III	WIR1015	V0014938	MAC: 1, 2, 3	CL: C, S	IAC: PRTN-1, VIIR-1, VIIR-2	Ref: DoDD 8530.2
Vulnerability: Disposal of Wireless email device is not compliant.						
The IAO will ensure that prior to disposing of a wireless email handheld PED (e.g. sold, transferred to another DoD or other government agency, etc.), the procedures found in the appropriate wireless push email system checklist are followed. For BlackBerry handhelds, the procedure listed in Appendix B will be followed. **Check**: Interview the IAO. Verify proper procedures are being followed and the procedures are documented.						
Comments:						

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR1070 Use only the BES email solution.

CAT I	WIR1070	V0014021	MAC: 1, 2, 3	CL: S, P	IAC: ECSC-1	Ref: Wireless STIG
Vulnerability: BlackBerry Enterprise Server is not used						
The IAO will ensure only the BES email solution (version 4.0.0.4 (version 4.0 with Service Pack 2) or later) is used. The BlackBerry desktop redirector, BlackBerry Connect, and Internet solutions are not authorized for use. **Check**: 1. Interview IAO and BlackBerry system administrator. Verify that the BES is part of the site's BlackBerry architecture and the site uses BES version 4.0.0.4 or later. From the BlackBerry Manager applet, select Help to view the version number. 2. Check for correct IT policy setting to disable other messaging services. Reviewed as part of WIR1250 check. The reviewer should lower to a CAT II or III **if only** configuration settings designated as CAT II or III **remain in an Open status** and all other requirements in this check are met.						
Comments:						

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR1080 Install Wireless Email servers using an approved architecture.

CAT I	WIR1080	V0014022	MAC: 1, 2, 3	CL: S, P	IAC: ECSC-1	Ref: Wireless STIG

Vulnerability: Network architecture is not compliant

The IAO will ensure that the Wireless Email system is set up with the required components and software installed on the handheld device.

For BlackBerry system:
The system will be installed and configured using either the BlackBerry DMZ Solution or the BlackBerry Firewall Solution as follows. (See Section 3.14 for firewall configuration requirements).

If the **BlackBerry DMZ Solution** architecture is used, apply the following policies. (See Figure 2.1 for example architecture)

– The BES and other systems used to host BlackBerry services (e.g., email server and Lightweight Directory Access Protocol (LDAP) server) is protected behind at least one firewall but remains outside the intranet firewall (in a DMZ).

– BlackBerry systems are not authorized to initiate communications to Intranet clients and/or servers. Only sessions from Intranet clients and/or servers are authorized to initiate connections to the systems used to host BlackBerry services in the DMZ.

– The BES is only authorized to communicate with systems in the DMZ that host BlackBerry services (e.g., email server and LDAP server) and only using the authorized ports and protocols.

– The BES is only authorized to communicate outside the DMZ with specified BlackBerry services (e.g., BlackBerry SRP server, OCSP, SSL/TLS, HTTP, and LDAP). All outbound connections are initiated by the BlackBerry system and/or service.

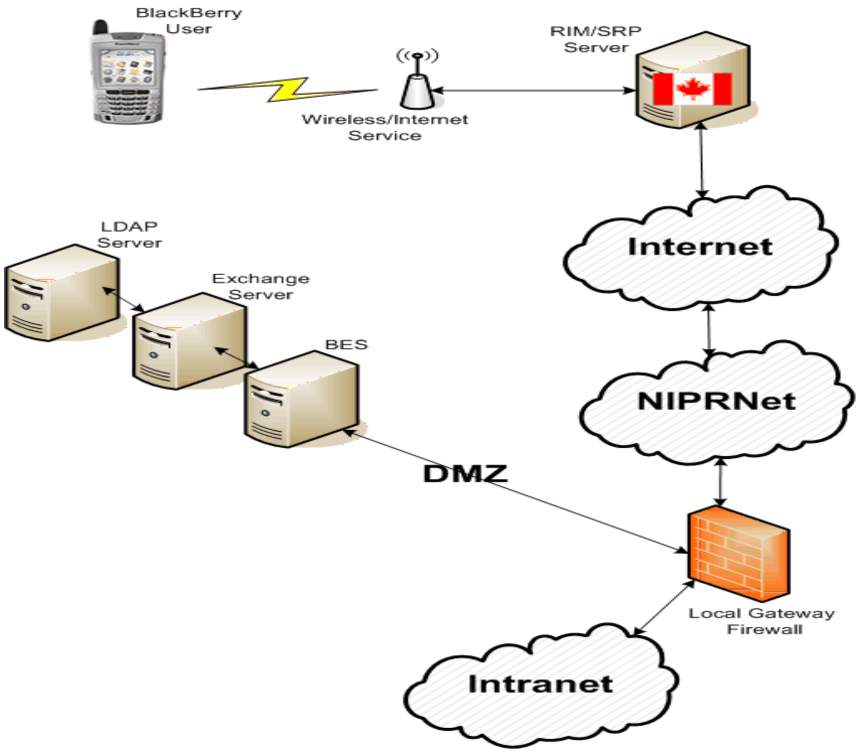


Figure 2-1. Example BlackBerry DMZ Network Architecture

WIR1080 (continued from previous page)
If the **BlackBerry Firewall Solution** architecture is used (See Figure 2.2 for example architecture), apply the following policies. (See Section 3.14 for firewall configuration requirements). – The BES and all other systems used to host BlackBerry services (e.g., email server and LDAP server) are protected behind a corporate firewall. – The BES will have a host based firewall (e.g., McAfee Personal Firewall, Norton Personal Firewall) and/or dedicated hardware firewall (e.g., Cisco, Netscreen) with the following required statements or rules. (See Wireless STIG BlackBerry Checklist version 5.1 or later for configuration requirements.) o Internal traffic from the BES is limited to internal systems used to host the BlackBerry services (e.g., email and LDAP servers). Communications with other services, clients, and/or servers are not authorized. o Internet traffic from the BES is limited to only those specified BlackBerry services (e.g., BlackBerry SRP server, OCSP, SSL/TLS, HTTP, and LDAP). All outbound connections are initiated by the BlackBerry system and/or service.

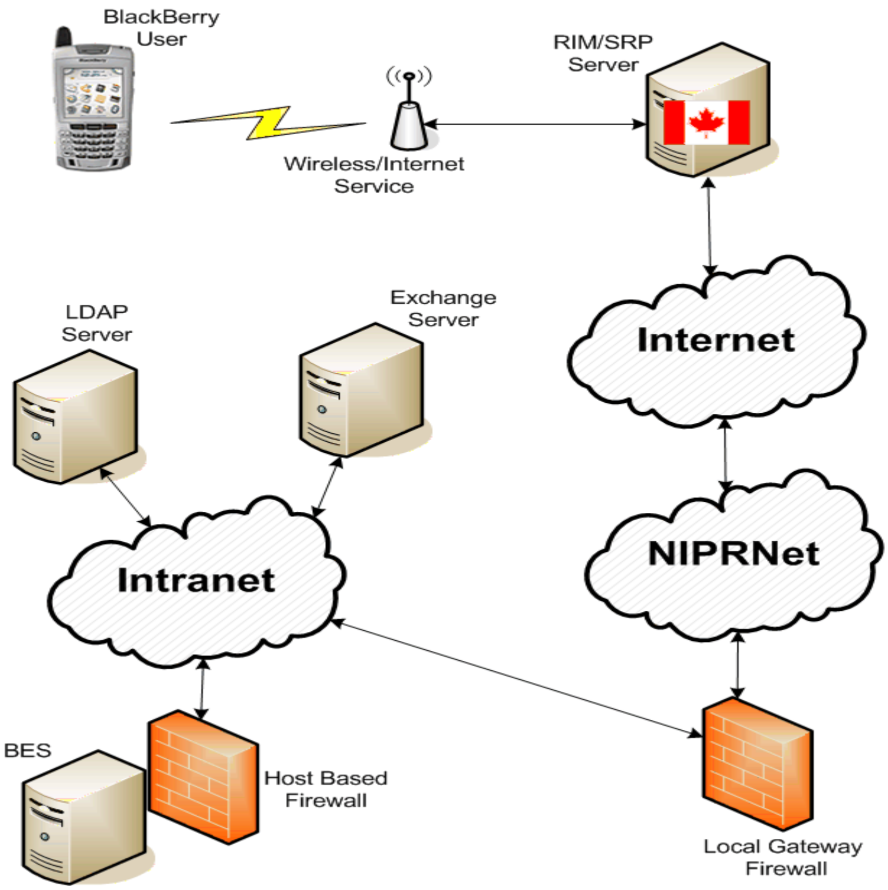


Figure 2-2. Example BlackBerry Firewall Network Architecture

WIR1080 (continued from previous page)

Check: Interview the IAO and system administrator and review system network diagrams..

For BlackBerry system:
Verify that logical connectivity complies with the requirements of one of the approved architectures (the drawings in Figure 2.1 or Figure 2.2 (of the BlackBerry Checklist) show example architectures). Other similar architectures may also meet the approved architecture requirements.

Verify the firewall configuration meets approved architecture configuration requirements (or have the network reviewer do the review of the firewall).

Mark as a finding if a BES is not used. Mark as a finding if the BES is used but the required firewalls, host servers and communication flow is not configured in accordance with the DMZ or firewall architecture.

Comments:

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR1090 Required actions if wireless email handheld is lost or stolen.

CAT II	WIR1090	V0003544	MAC: 1, 2, 3	CL: S, P	IAC: ECSC-1	Ref: Wireless STIG

Vulnerability: Wireless email devices are not deactivated if lost/stolen.

The IAO will ensure the wireless email system administrator sends a “Wipe” or “Kill” command to the device and removes the device from the wireless email management server when a wireless email device is reported lost or stolen.

If a wireless email device is lost or stolen, the device must be immediately disabled to prevent unauthorized use or access. Once the device is deemed unrecoverable, the device should be permanently removed from the server and SA should contact the service provider to cancel the service.

Check:
For BlackBerry system:

Two actions required:

1. User trained to immediately notify the IAO and/or BlackBerry administrator when a BlackBerry is lost or stolen
2. BlackBerry Administrator immediately sends a Kill Handheld command when notified of a lost or stolen device.

Review written policies and end user training materials. Verify that proper procedures are followed when devices are lost or stolen. If a BlackBerry device is lost or stolen, the device must be immediately disabled to prevent unauthorized use or access. Once the device is deemed unrecoverable, the device should be permanently removed from the server and SA should contact the service provider to cancel the service.

Comments:

Open	□	Not a Finding	□	Not Reviewed	□	Not Applicable	□

WIR1100 Authenticated login procedures to unlock a wireless email device

CAT II	WIR1100	V0003545	MAC: 1, 2, 3	CL: S, P	IAC: ECSC-1	Ref: Wireless STIG

Vulnerability: Wireless email device not protected by authentication.

The IAO will ensure the wireless email device is protected by authenticated login procedures to unlock the device. Either CAC or PIN authentication is required.

When PIN authentication is used, the following procedures will be enforced.

- The device password /PIN is set to five or more characters. The system security policy must be configured to enforce this policy. If five characters are used, both a letter (lower or upper case) and a number must be used in all device passwords (the wireless email server must be configured to enforce this policy). If six or more characters are used, only numbers may be used for the password. It is recommended that eight or more characters be used.

- The number of incorrect passwords entered before a device wipe occurs is set to 10 or less. The system security policy must be configured to enforce this policy.

- The password is changed at least every 90 days. The system security policy must be configured to enforce this policy.

Check: Interview the IAO and administrator.
1. Verify CAC authentication or PIN authentication is used.
2. If PIN authentication is used, verify correct settings. These policies are given in Appendices B and are reviewed as part of check WIR1250. The reviewer must raise this to a CAT I finding if **any** configuration setting designated as CAT I **remains in an Open status**. The reviewer should lower to a CAT III **if only** configuration settings designated as CAT III **remain in an Open status**.

Comments:

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR1110 Password Keeper configuration must be compliant.

CAT I	WIR1110	V0011865	MAC: 1, 2, 3	CL: S, P	IAC: ECSC-1	Ref: Wireless STIG

Vulnerability: Password Keeper configuration is not compliant

The IAO will ensure that when the Password Keeper is enabled on the BlackBerry device, the DAA has reviewed and approved its use, and the application is configured to enforce the following password rules.

- Require use of eight or more characters. The Password Keeper must be configured to enforce this policy.

- Set the number of incorrect passwords entered before a device wipe occurs to 10 or less.

- Set local policy to require a change of password at least every 90 days.

Check: Interview the IAO.
1. Ask if users are allowed to use Password Keeper on their handheld devices. If Password Keeper is used, review DAA approval documentation.

2. Work with the IAO to view the Password Keeper configuration on a sampling of BlackBerry devices using this application. On BlackBerry, go to Applications/Password Keeper. (The Password Keeper icon may also be installed directly on the BlackBerry home screen.)

3. Verify that users are trained on password change requirement by reviewing user agreement or training materials.

Comments:

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR1120 Wireless email devices are set to lock after 15 minutes or less of inactivity.

CAT II	WIR1120	V0007077	MAC: 1, 2, 3	CL: S, P	IAC: ECSC-1	Ref: Wireless STIG

Vulnerability: Wireless email devices not set for a 15-minute lockout

The IAO will ensure all wireless email devices are set to lock (timeout) after 15 minutes or less of inactivity.

Check:

For BlackBerry system
Work with the SA to review the configuration of the BES IT Policy rules. Reviewed as part of WIR1250 check. The reviewer should lower to a CAT III **if only** configuration settings designated as CAT III **remain in an Open status** and all other requirements in this check are met.

Reviewers may also check this setting on a sample of BlackBerry devices (in addition to checking the IT Policy rule setting): Options/Security Options/General Settings/Security Timeout.

Comments:

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR1130 CAC authentication requirements with BlackBerry MDS.

CAT I	WIR1130	V0007078	MAC: 1, 2, 3	CL: S, P	IAC: ECSC-1	Ref: Wireless STIG

Vulnerability: Smart card PKI digital certificate authentication is not enabled

The IAO will ensure when a BlackBerry Mobile Data Service (MDS) on the BlackBerry Enterprise Server (BES) is used to provide user access to DoD network web servers, CAC PKI certificate based authentication is implemented on the web server for all BlackBerry users.

Check: Interview the IAO and BlackBerry Administrator. Verify PKI authentication has been implemented at any internal network application or web server that BlackBerry users have been granted access to.

Comments:

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR1140 Bluetooth usage must be compliant.

CAT II	WIR1140	V0014198	MAC: 1, 2, 3	CL: S, P	IAC: ECSC-1	Ref: Wireless STIG

Vulnerability: Wireless Bluetooth configuration not compliant

The IAO will ensure a wireless email device, which has a Bluetooth radio, applies the following Bluetooth controls.

- Bluetooth data transmissions (e.g. syncing to the desktop or transfer of data files) on BlackBerry devices is disabled except for the Bluetooth CAC reader (i.e., Bluetooth Smart Card Reader (SCR)). Only DISA tested and approved Bluetooth SCRs may be used.

- Bluetooth for voice transmissions (e.g. Bluetooth ear bud) is not authorized. Both the Bluetooth Handsfree and Headset profiles are disabled by BES IT Policy configuration. Users should use wired handsfree devices.

Check:
For BlackBerry system:
Check the BES IT Policy. Reviewed as part of WIR1250 check.
The reviewer must raise this to a CAT I finding if **any** configuration setting designated as CAT I **remains in an Open status**. The reviewer should lower to a CAT III **if only** configuration settings designated as CAT III **remain in an Open status**.

Comments:

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR1150 Bluetooth Smart Card Reader usage must be compliant.

CAT III	WIR1150	V0011866	MAC: 1, 2, 3	CL: S, P	IAC: ECSC-1	Ref: Wireless STIG
Vulnerability: Wireless email device Bluetooth SCR usage not compliant						

For BlackBerry system:
The IAO will ensure that when RIM Bluetooth Smart Card Readers (SCR) or the Apriva Bluetooth SCR is used in the organization, the following procedures will be followed.

– BlackBerry Handheld Software version 4.1.0.294 or later is used on all BlackBerry devices.

– Only the RIM Bluetooth SCR or the Apriva BT 100-C Bluetooth SCR are used with RIM BlackBerry devices. The SCR is not used with PCs, cell phones, PDAs, or non-RIM PDAs with BlackBerry software installed (BlackBerry Connect).

– When the RIM Bluetooth SCR is used as a PC SCR, the requirements listed in section 3.18 of the Wireless STIG BlackBerry Checklist must be followed. Required version of BlackBerry Smart card reder software application on the Bluetooth enabled PCs is v4.2.0.88 or later. Required version of SCR operating system is v1.5.1 (platform 1.5.0.81) or later. Earlier versions will not be used for PC connections. Separate BlackBerry Account Groups should be created: one for users that are authorized to use the RIM BlackBerry Smart Card Reader with their PCs and one for users that are NOT authorized to use the RIM BlackBerry Smart Card Reader with their PCs (or do not have a RIM BlackBerry Smart Card Reader).

– Only the RIM Bluetooth SCR and the Apriva BT 100-C Bluetooth SCR are authorized for use with the BlackBerry. Bluetooth SCRs from other manufacturers have not undergone a DoD security evaluation and are not approved by DISA.

– Separate BlackBerry account groups are set up for users that use the SCR and for users that do not use the SCR. The IT Policy rules for the Bluetooth group policy will be set as indicated in Table C-1 for each BlackBerry account group.

– Users are trained how to perform the following:

- Perform secure pairing immediately after the SCR is reset.
- Select a strong reader connection password (during initial pairing of the SCR with a Blackberry, the user is required to select a connection password). Select at least an eight character password.
- Accept only Bluetooth connection requests from devices they control.
- Reject Pass Key entry requests for devices they have already paired with using the escape button.
- Monitor Bluetooth connection requests and activity in order to detect possible attacks and unauthorized activity.

- Change Bluetooth device property **Trusted** field to "**Ask**." This property is set on the BlackBerry device in the Bluetooth Device Properties immediately after the Bluetooth pairing connection alert. To check (or change), do the following: On the BlackBerry, Select Options/Bluetooth/Smart Card Reader/Device Properties
- NOT check the "Don't ask this again" alert box during pairing, when a connection alert is received. Checking this box disables connection alerts with that device.

Check: Interview the IAO and wireless email system administrator.

For BlackBerry system:

1. Verify that the BlackBerry SA places users with or without card readers in separate BlackBerry account groups.

2. Review training materials or sample user agreements to verify users are trained on secure pairing procedures for the card reader.

3. View a sampling of BlackBerry devices or the site's configuration document to verify the device property **Trusted** field is set to "**Ask**" and that the authorized version of the BlackBerry Handheld Software is installed. Check by selecting Options/Bluetooth/SCR/Device Properties on a BlackBerry device that is paired with a SCR.

4. Verify that if the RIM BlackBerry Smart Card Reader is used as a PC SCR the following requirements are met:

– The DAA has approved the use of the RIM BlackBerry Smart Card Reader with site PCs. Have the IAO provide documentation showing DAA approval (letter, memo, SSP, etc.)
– Verify separate BlackBerry Account Groups have been created: one for users that are authorized to use the RIM BlackBerry Smart Card Reader with their PCs and one for users that are NOT authorized to use the RIM BlackBerry Smart Card Reader with their PCs (or do not have a RIM BlackBerry Smart Card Reader). (Required BES setting are reviewed during WIR1250 check.)

(Note: Recommend 3 BlackBerry account groups be created:
1. BlackBerry users without a smart card reader.
2. BlackBerry users with a smart card reader, but not authorized to use the smart card reader to connect to their PC.
3. BlackBerry users with a smart card reader and authorized to use the smart card reader to connect to their PC.)

– Interview the IAO and SA and verify that the RIM BlackBerry SCR is not used with Windows Vista. Only Windows XP SP2 is approved at this time. BlackBerry users with Vista on their PCs must be put in the BlackBerry users group not authorized to use the BlackBerry SCR with their PCs.

- Interview the IAO and verify Bluetooth radios are disabled in all PCs where users do not have a RIM BlackBerry Smart Card Reader (Bluetooth radios will be disabled either by removing the radio from the PC and/or by Windows group policy).
- Interview the IAO to verify only Bluetooth Class 2 or 3 radios must be used by the PC. Class 1 (100 mW) Bluetooth radios are not allowed. (Note for IAOs: To determine the “class” rating of the Bluetooth radio, look under the specification section of the Bluetooth Network Interface Card manual, which can be downloaded from the laptop vendor’s web site or the Bluetooth dongle vendor’s web site.)
- Verify only RIM BlackBerry Smart Card Reader operating system 1.5.1 build 81 or later will be installed on the smart card reader and BlackBerry Smart Card Reader software application version 4.2.0.88 or later will be installed on Bluetooth enabled PCs.
  (Start>Control Panel>Add or Remove Programs>Select "Blackberry Smart Card Reader v1.5.1" and click the "Click here for support information" link. Verify that the "Version:" field says "4.2.0.88 (Platform 1.5.0.81)."
- Verify the RIM Bluetooth Lockdown tool is installed.
  Start>Control Panel>Add or Remove Programs> Select "Blackberry Smart Card Reader v1.5.1" and click the "Change/Remove" button. In the first pop-up dialog box click "Next >" button. In the next dialog box verify that "Modify" is selected and click the "Next >" button. In the next dialog box click the "Next >" button. In the next dialog box ("Restrict Bluetooth Functionality"), verify that the checkbox is checked. **Click the "Cancel" button and cancel installation.**
- Interview the IAO and verify the site Windows group security policy is set to restrict the capability of the PC user to disable, remove, or change the configuration of the RIM Bluetooth Lockdown tool.
- Verify all PC users with administrative account rights to their PC have been trained to never disable the RIM Bluetooth Lockdown tool on their PC. Ask for training documentation and training completion record (this training can be included in the User Agreement). (PC Administrators should NEVER change any Bluetooth settings followings implementation of Bluetooth lockdown.)

5. Required BES setting are reviewed during WIR1250 check. The reviewer must raise this to a CAT II finding if **any** configuration setting designated as CAT II **remains in an Open status**.

Comments:

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR1160 Secure wireless email servers using operating system STIG.

CAT II	WIR1160	V0014199	MAC: 1, 2, 3	CL: S, P	IAC: ECSC-1	Ref: Wireless STIG

Vulnerability: Operating system for wireless email server host is not compliant.

For BlackBerry system:

The IAO will ensure that all host servers and computers where BlackBerry services are installed (e.g., BES, email server, and LDAP server) and hardened in accordance with the appropriate operating system STIG.

Check: Work with the OS reviewer or check VMS for last review of the host computer asset. Verify that there are not outstanding CAT I findings associated with the host server.

Mark as a finding if CAT I findings are open for the host computer operating system or if a SRR or site self-check was not performed for the host computer.

For BlackBerry system:

Asset to check: BlackBerry Enterprise Server

Comments:

Open	□	Not a Finding	□	Not Reviewed	□	Not Applicable	□

WIR1170 Comply with provisioning requirements for new/re-issued wireless email devices.

CAT II	WIR1170	V0011868	MAC: 1, 2, 3	CL: S, P	IAC: ECSC-1	Ref: Wireless STIG

Vulnerability: Wireless email devices wipe procedures are not compliant

For BlackBerry system:

1. The IAO will ensure that a BlackBerry system administrator performs a “Wipe (or Nuke) Handheld” command on all new or reissued BlackBerry handheld devices and that all BlackBerry, wireless carrier, and system software is reloaded on the BlackBerry from a trust source and the site BlackBerry IT policy is pushed to the device before issuing it to DoD personnel and placing the device on a DoD BlackBerry network.

2. When wireless activation is performed, the activation password is passed to the user in a secure manner (e.g., activation password is encrypted and emailed to an individual).

Check: Interview the IAO. Verify required procedures are followed.

Comments:

Open	□	Not a Finding	□	Not Reviewed	□	Not Applicable	□

WIR1180 Do not allow users to install or remove applications.

CAT I	WIR1180	V0011869	MAC: 1, 2, 3	CL: S, P	IAC: ECSC-1	Ref: Wireless STIG

Vulnerability: Users allowed to update or remove applications

The IAO will ensure that BlackBerry users do not install or remove applications and/or software on their handheld device unless under the direction and supervision of an authorized BlackBerry system administrator.

Check: Work with the SA to verify this requirement by reviewing the following:

For BlackBerry system:

1. IT Policy rules set in the BES. Reviewed as part of WIR1250 check. The reviewer should lower to a CAT II **if only** configuration settings designated as CAT II **remain in an Open status** and all other requirements in this check are met.

2. Verify an application control policy has been set on the BES to either block all third party applications or permit only specific DAA approved applications. See Section 3.8 of this checklist for instructions on how to perform this check.

3. If specific third party applications are approved for use by BlackBerry users, verify an application control policy has been set for each approved application that specifies assigned permissions for the application. All application permission rules should be set to “Not Permitted” by default and set to “allowed” or “Prompt User” only if required for application operation. See Table 3.7 of this checklist for additional information.

Comments:

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR1190 Do not install Onset Technologies Metamessage software.

CAT I	WIR1190	V0011870	MAC: 1, 2, 3	CL: S, P	IAC: ECSC-1	Ref: Wireless STIG

Vulnerability: Metamessage is installed on BlackBerry devices.

The IAO will ensure Onset Technologies Metamessage software is not installed on DoD BlackBerry devices or on the BES.

Check:

1. Have the BlackBerry Administrator show that there is no application control policy for this application. See Section 3.8 of this checklist for instructions on how to perform this check.

2. Check a sample of BlackBerry devices (Options/Advanced Options/Applications) to ensure the application is not loaded on the device.

The Metamessage application allows the user to open and create Microsoft Office files such as MS Word or Excel attachments or documents. These documents can then be sent via email, saved, or printed. This application presents a security risk and is not allowed for use in DoD. Verify this software application is not used by interviewing the IAO or reviewing a sampling of the devices.

Comments:

Open	□	Not a Finding	□	Not Reviewed	□	Not Applicable	□

WIR1200 Digitally sign wireless email emergency and/or critical email notifications.

CAT II	WIR1200	V0011871	MAC: 1, 2, 3	CL: S, P	IAC: ECSC-1	Ref: Wireless STIG

Vulnerability: Emergency or critical messages not signed

The IAO will ensure that all wireless email emergency and/or critical email notifications are digitally signed and verified to ensure the authenticity of the sender.

Check: Interview the IAO

For BlackBerry system:
.

1. Check the BES IT policy rule for the S/MIME Application policy group (checked as part of WIR1250). The reviewer should lower to a CAT III **if only** configuration settings designated as CAT III **remain in an Open status** and all other requirements in this check are met.

2. Verify that S/MIME is configured such that users may sign messages.
   Check a sample of BlackBerry devices:

   – Verify S/MIME application and Smart Card Reader drivers are installed on the device: (Options/Advanced Options/Applications).

   – Verify Certificates are configured on the BlackBerry:
   (Options/Security Options/Certificate Servers) – GDS should be listed;
   (Options/Security Options/Certificate) - DoD Root certificates should be listed
   (Options/Security Options/S/MIME) – user’s public keys should be loaded.

3. Verify that users are trained on how to sign messages on the BlackBerry and that users are trained to sign emergency and critical email notifications.

4. Verify that if soft certs are used on the Windows Mobile device, the DAA has approved their use (letter, memo, SSP, etc.).

Comments:

Open	□	Not a Finding	□	Not Reviewed	□	Not Applicable	□

WIR1210 Configure wireless email auto signature as required.

CAT III	WIR1210	V0011872	MAC: 1, 2, 3	CL: S, P	IAC: ECSC-1	Ref: Wireless STIG

Vulnerability: Signature message is not compliant.

The IAO will ensure that if wireless email auto signatures are used, the signature message does not disclose that the email originated from a mobile device (e.g., "Sent From My Wireless Handheld").

Check:
For BlackBerry system:

1. Note that the site can disable the use of auto signature via an IT policy rule (checked as part of WIR1250).
2. If allowed, check a sample of user PC BlackBerry desktop Manager:

   - Open "Desktop Manager on user's PC.
   - Double-click "Redirector Settings"
   - Check the contents of "Auto Signature" text box to verify compliance.

Comments:

Open	□	Not a Finding	□	Not Reviewed	□	Not Applicable	□

WIR1220 If Text Messaging is used, enable security.

CAT II	WIR1220	V0011873	MAC: 1, 2, 3	CL: S, P	IAC: ECSC-1	Ref: Wireless STIG

Vulnerability: Text Messaging is not compliant.

The IAO will ensure security requirements for Text messaging (Short Message Service (SMS), Multi-media Messaging Service (MMS), Pin-To-Pin messaging, and other text messaging services) are followed as described in the appropriate wireless email system checklist.

Check:

For BlackBerry system:

1. Verify S/MIME function enabled for PIN-to-PIN messaging (checked as part of WIR1250 check).

2. Verify S/MIME Support Package is installed. Check a sample of BlackBerry devices (see WIR1200, #3 for the procedure).

3. If SMS is used, interview the IAO and check IA awareness training material to ensure training includes SMS/MMS security issues.

4. Verify MMS is not enabled on the BES. (checked as part of WIR1250 check).

The reviewer should lower to a CAT III **if only** configuration settings designated as CAT III **remain in an Open status** and all other requirements in this check are met.

Comments:

Open	□	Not a Finding	□	Not Reviewed	□	Not Applicable	□

WIR1240 The wireless carrier Internet browser is disabled.

CAT II	WIR1240	V0011875	MAC: 1, 2, 3	CL: S, P	IAC: ECSC-1	Ref: Wireless STIG

Vulnerability: BES MDS is not used for Internet browsing.

The IAO will ensure that all Internet browsers are disabled and removed from the BlackBerry device accept for the BlackBerry internet browser.

Check:

1. Review a sampling of handheld devices and verify that the Wireless Carrier’s internet browser, web portal browser, and all other browsers (Yahoo, etc.) are not installed on the BlackBerry device. The only browser installed should be the BlackBerry browser. Go to the BlackBerry device Home screen and check Options/Advanced Options//Browser.

2. Check that other browsers are not allowed by IT policy configuration (checked as part of WIR1250 check). The reviewer should lower to a CAT III **if only** configuration settings designated as CAT III **remain in an Open status** and all other requirements in this check are met.

Comments:

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR1250 Implement wireless email servers and handheld configuration settings.

CAT II	WIR1250	V0011876	MAC: 1, 2, 3	CL: S, P	IAC: ECSC-1	Ref: Wireless STIG

Vulnerability: The wireless email server and handheld device configurations are not compliant

The IAO will ensure that all required wireless email server and handheld device configuration settings are implemented.

For BlackBerry system:
See requirements listed in Section 3 and Appendices C, D, and G.

Check:

For BlackBerry system:

Verify the BlackBerry administrator has used the configuration settings list in Section 3 and Appendix C of the *Wireless STIG, BlackBerry Security Checklist* as follows:

1. Determine if Push or Pull applications on the network are configured to connect to the BES. If yes, see Section 3.3.4 for the required access control policies for the Push and Pull applications. Verify the access control policies have been set for the MDS connection on the BES (CAT III finding if not set).
   - In the **BlackBerry Manager**, select a **BlackBerry MDS Connection Service** in the left pane
   - On the **Connection Service** tab, select **Edit Properties**
   - Select **Access Control**

2. Appendix C. Verify all required IT policy rules have been set on the BES. Open findings should marked be against the check number listed in the table for the IT policy rule found to be in “Open” status.

3. Appendix D. A sample of BlackBerry devices should be checked. Open findings should marked be against the check number listed in the table for the IT policy rule found to be in “Open” status.

4. Appendix G. If team or Group BlackBerrys are used, ensure procedures in Appendix G have been followed.

The reviewer must raise this to a CAT I finding if **any** configuration setting designated as CAT I **remains in an Open status**. The reviewer should lower to a CAT III **if only** configuration settings designated as CAT III **remain in an Open status**.

Note: Open checks in Appendix C & D should be marked against the check number listed in the table for the “Open” IT Policy rule.

Comments:

Open		Not a Finding		Not Reviewed		Not Applicable	

WIR1260 Configure Automatic Master Key generation on the BES.

CAT I	WIR1260	V0011877	MAC: 1, 2, 3	CL: S, P	IAC: ECSC-1	Ref: Wireless STIG

Vulnerability: Master Key generation is not configured

The IAO will ensure that automatic Master Key generation is configured on the BES.

Check:

1. Check this requirement during the review of the IT Policy rules set in the BES. Checked as part of WIR1250 check. The reviewer should lower to a CAT III **if only** configuration settings designated as CAT III **remain in an Open status** and all other requirements in this check are met.

2. Work with the BlackBerry SA to view the BlackBerry server properties, General tab. In the Supported Encryption Algorithms section verify that AES, 3DES or both are selected as shown in Section 3.6 of this checklist. The configuration must also be set to generate keys automatically (every 30 days).

Comments:

Open	□	Not a Finding	□	Not Reviewed	□	Not Applicable	□

WIR1270 BlackBerry device must be cradled once every 30 days.

CAT II	WIR1270	V0011879	MAC: 1, 2, 3	CL: S, P	IAC: ECSC-1	Ref: Wireless STIG

Vulnerability: BlackBerry devices are not cradled every 30 days.

The IAO will ensure that local policies include requiring the BlackBerry device to be cradled once every 30 days. This will ensure that the BlackBerry receives updated Master Keys and software updates on a frequent basis.

Check:

1. Interview the IAO.

2. Review written policies or training material. Verify that users are trained to cradle the BlackBerry handheld device every 30 days or less.

3. Check that IT Policy Rules are set to notify user when software updates are available. Checked as part of WIR1250 check. The reviewer should lower to a CAT III **if only** configuration settings designated as CAT III **remain in an Open status** and all other requirements in this check are met.

Comments:

Open	□	Not a Finding	□	Not Reviewed	□	Not Applicable	□

WIR1280 Data-at-rest encryption is enabled on all wireless email devices.

CAT III	WIR1280	V0012164	MAC: 1, 2, 3	CL: S	IAC: ECSC-1	Ref: Wireless STIG

Vulnerability: Data-at-Rest encryption is not enabled

The IAO will ensure that Data-at-Rest encryption is enabled on all wireless push email devices.

For BlackBerry system:

NOTE**:** When Content Protection is enabled, the BES system administrator *cannot* remotely unlock a BlackBerry device and remotely reset the device password. RIM is scheduled to release a BES update in late 2007 (November) to provide remote device unlock / password reset when Content Protection is enabled.

Check:
For BlackBerry system:

1. Work with BlackBerry SA to verify that IT Policy rules are set in accordance with Appendix C. Checked as part of WIR1250 check.

2. In addition to checking the IT Policy Rule settings, a sample on BlackBerry devices may also be checked as follows: Options/Security Options/General Settings/Content Protection.

Comments:

Open		Not a Finding		Not Reviewed		Not Applicable	

3. BES SECURITY RELATED CONFIGURATIONS

The following paragraphs describe "Required" and "Optional" security related configuration settings for the BlackBerry Enterprise Server, 4.0/4.1.

NOTE*:* Vulnerability Severity Codes are listed in the following paragraphs only if the configuration settings described are not controlled by an IT Policy rule and are not listed in Appendix C or D.

3.1 Creating IT Policies

References:

- BlackBerry Enterprise Server for Microsoft Exchange, Version 4.1.4, System Administration Guide, page 36.
- BlackBerry Enterprise Server, All released versions (4.1.4 and earlier), Policy Reference Guide (Version 16), 10 July 2007.

IT policies are a collection of rules that are used by the BES to define how mail is handled and what functions are available on the BlackBerry device. There are over 300 possible policy rules, which are grouped into 31 policy groups. Table C.1, BES IT Policy Rules, lists all required and optional BlackBerry IT policy settings which are directly or indirectly related to the security of the BlackBerry system. Table D.1, BlackBerry Handheld Software 4.0-4.2 Configuration Settings, lists device settings related to the security of the device.

All new users are assigned to the base or "default" policy. The BES administrator can define customized IT policies and assign users to specific policies based on their roles, jobs, or other needs of the organization.

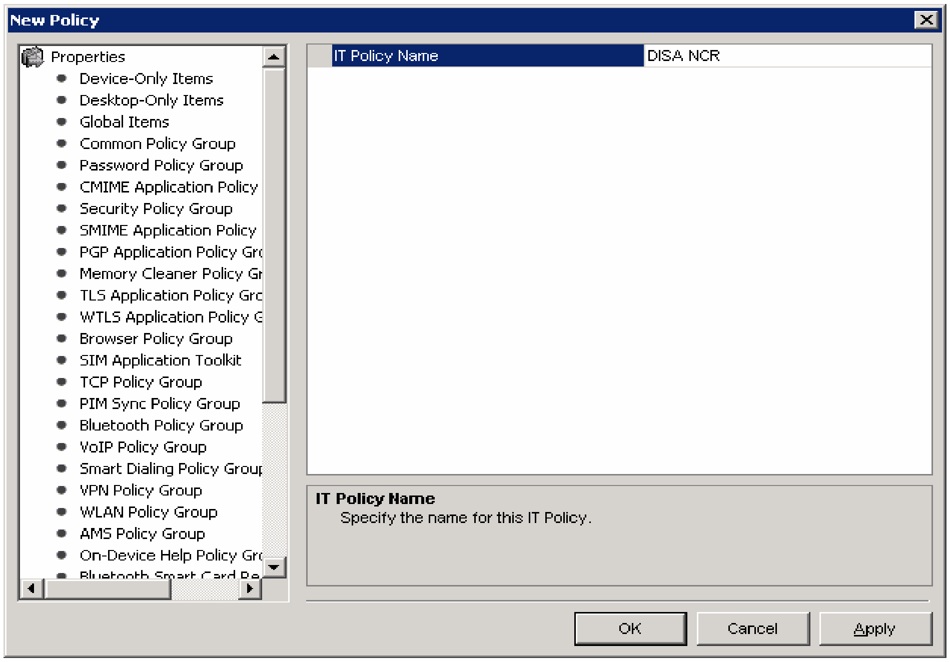
Research In Motion recommends that after installing the BES, the BES administrator should create a new "blank" IT policy that has the exact same settings as the factory default BES policy (for example, name this policy "BES Factory Settings"). The BES administrator should then configure the "default" policy to meet organizations operational and security requirements. After following these procedures, if the BES is ever inadvertently reset to the system default IT policy, the BES will continue to meet the organizations minimum requirements and the factory default policy will also be available for system troubleshooting, if needed.

NOTE*:* Users can only be members of one IT policy at a given time.

Steps to create a new IT policy.

1. In the BlackBerry Manager, in the left pane, click **BlackBerry Domain.**.
2. On the **Global** tab, click **Edit Properties**.
3. Click **IT Policy**.
4. In the **IT Policy Administration** section, double-click **IT Policies.**
5. Click **New**.
6. Double-click **IT Policy Name**
7. Type a name for the new policy.

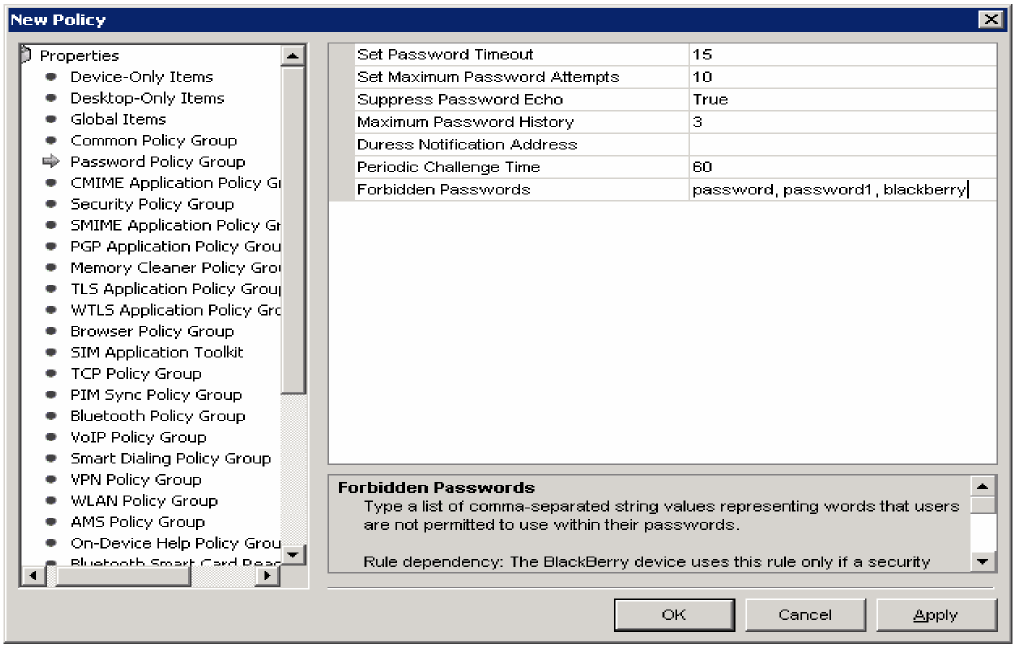
8. Configure the IT policy rules by performing the following steps:
    a. In the left pane, click a policy group.
    b. In the right pane, double-click the IT policy rule.
    c. Set a value for the IT policy rule.
9. Click **OK**.



IT Policy Name	DISA NCR

IT Policy Name
Specify the name for this IT Policy.

Figure 3-1. Screen Shot – Create new IT Policy



Set Password Timeout	15
Set Maximum Password Attempts	10
Suppress Password Echo	True
Maximum Password History	3
Duress Notification Address	
Periodic Challenge Time	60
Forbidden Passwords	password, password1 , blackberry

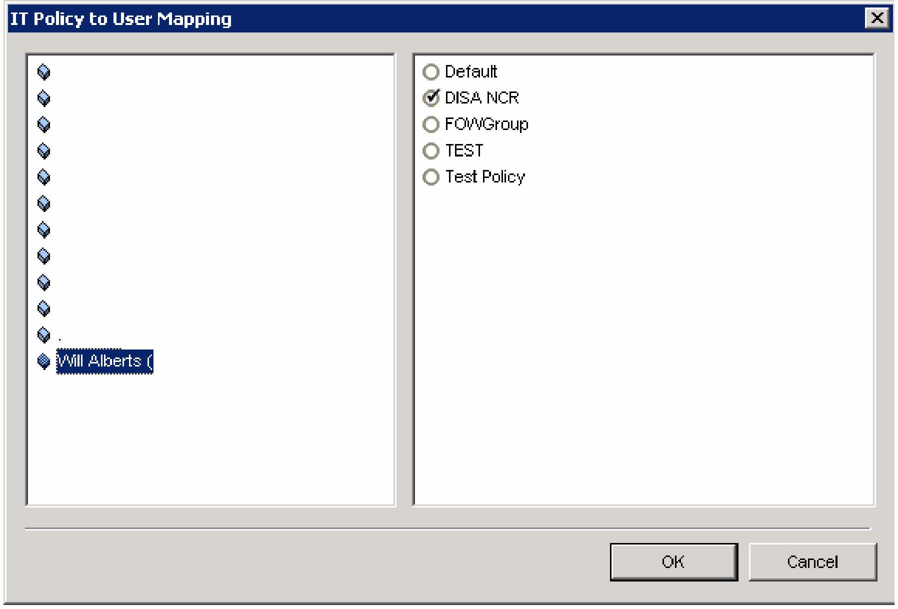
Forbidden Passwords
Type a list of comma-separated string values representing words that users are not permitted to use within their passwords.

Rule dependency: The BlackBerry device uses this rule only if a security

Figure 3-2. Screen Shot – Edit New IT Policy

After the new IT Policy is created, the next step is to assign users to the policy as follows.

1. In the BlackBerry Manager, in the left pane, click **BlackBerry Domain.**
2. On the Global tab, click **Edit Properties**.
3. Click **IT Policy**.
4. In the **IT Policy Administration** section, double-click **IT Policy to User Mapping**.
5. In the left pane, click a user account.
6. In the right pane, select the desired IT policy.
7. Click **OK**.



IT Policy to User Mapping

Will Alberts (

○ Default
● DISA NCR
○ FOWGroup
○ TEST
○ Test Policy

Figure 3-3. Screen Shot – Add Users to New IT Policy

3.2 Creating an Activation Password

Reference:

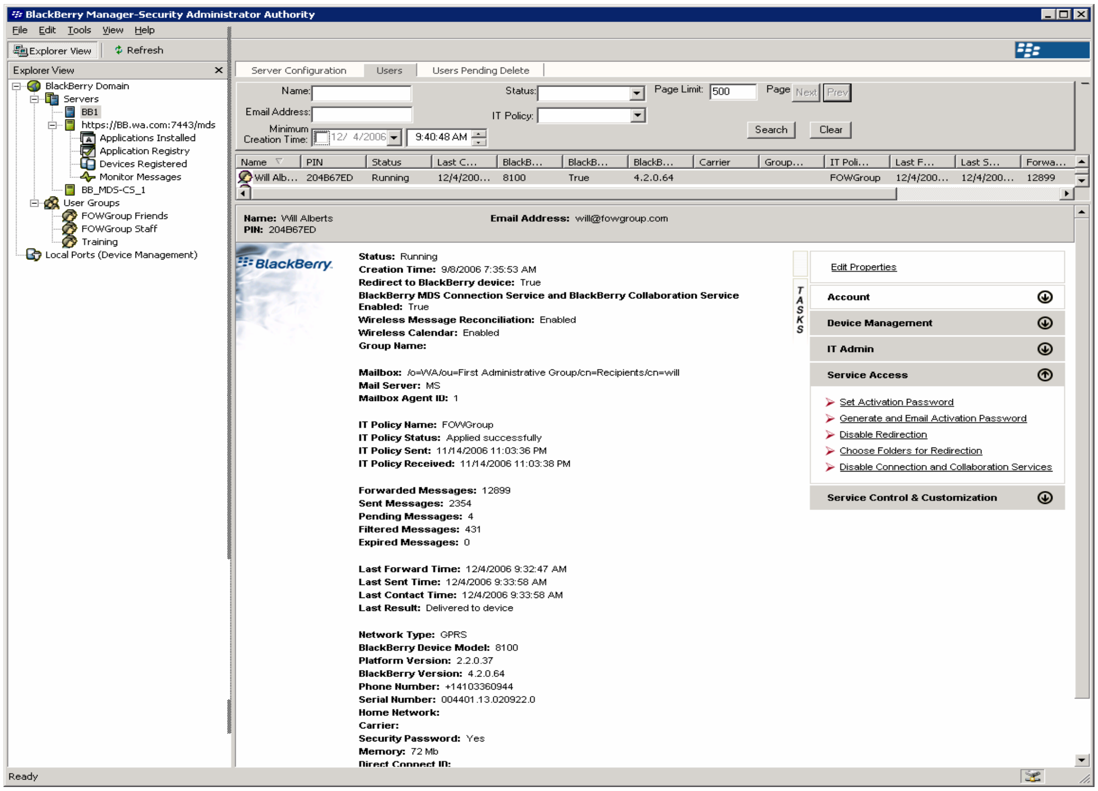
- BlackBerry Enterprise Server for Microsoft Exchange, Version 4.1.4, System Administration Guide, page 50.

When a BES administrator uses wireless enterprise activation, the administrator creates an Activation Password on the user’s BlackBerry account. A secure method must be used to provide this password to the user (e.g., similar to methods used to provide network passwords to network users).

Configuration or Action	Setting	
	Required	Optional
Activation Password	Passed to user by secure method	
Password Expiration Time		Recommend 12 hours or less

Setup the Activation Password using the following steps.

1. In the BlackBerry Manager, in the left pane, select a BES.
2. On the **Users** tab, select a user account.
3. Click **Service Access**
4. Click **Set Activation Password**
5. Type in shared password and retype it to confirm.
6. In the **Password Expires** box, type-in an expiration time.
7. Select **OK**.
8. Provide user password by secure method.



Page Limit: 500

Minimum Creation Time: 12/ 4/2006 9:40:48 AM

Name	PIN	Status	Last C...	BlackB...	BlackB...	BlackB...	Carrier	Group...	IT Poli...	Last F...	Last S...	Forwa...
Will Alb...	204B67ED	Running	12/4/200...	8100	True	4.2.0.64			FOWGroup	12/4/200...	12/4/200...	12899

Name: Will Alberts
PIN: 204B67ED
Email Address: will@fowgroup.com

Status: Running
Creation Time: 9/8/2006 7:35:53 AM
Redirect to BlackBerry device: True
BlackBerry MDS Connection Service and BlackBerry Collaboration Service Enabled: True
Wireless Message Reconciliation: Enabled
Wireless Calendar: Enabled
Group Name:

Mailbox: /o=WA/ou=First Administrative Group/cn=Recipients/cn=will
Mail Server: MS
Mailbox Agent ID: 1

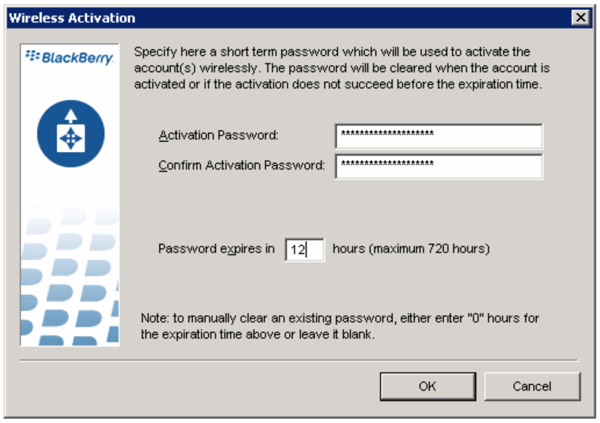
IT Policy Name: FOWGroup
IT Policy Status: Applied successfully
IT Policy Sent: 11/14/2006 11:03:36 PM
IT Policy Received: 11/14/2006 11:03:38 PM

Forwarded Messages: 12899
Sent Messages: 2354
Pending Messages: 4
Filtered Messages: 431
Expired Messages: 0

Last Forward Time: 12/4/2006 9:32:47 AM
Last Sent Time: 12/4/2006 9:33:58 AM
Last Contact Time: 12/4/2006 9:33:58 AM
Last Result: Delivered to device

Network Type: GPRS
BlackBerry Device Model: 8100
Platform Version: 2.2.0.37
BlackBerry Version: 4.2.0.64
Phone Number: +14103360944
Serial Number: 004401.13.020922.0
Home Network:
Carrier:
Security Password: Yes
Memory: 72 Mb
Direct Connect ID:

Figure 3-4. Screen Shot – Activation Password Setup



Specify here a short term password which will be used to activate the account(s) wirelessly. The password will be cleared when the account is activated or if the activation does not succeed before the expiration time.

Activation Password: *******************

Confirm Activation Password: *******************

Password expires in 12 hours (maximum 720 hours)

Note: to manually clear an existing password, either enter "0" hours for the expiration time above or leave it blank.

Figure 3-5. Screen Shot – Select Activation Password

3.3 Configuring MDS

References:

– BlackBerry Enterprise Server for Microsoft Exchange, Version 4.1.4, System Administration Guide, page 93.

The MDS is a BES component that provides secure data connections between the BlackBerry device, DoD servers, and Internet sites. The MDS acts as an intermediary between a BlackBerry device and applications, data, and services located on the DoD network to which the BES is connected and the Internet. Key MDS security issues are: authentication of the BlackBerry user; access control to only authorized services and connections; and encryption of data between the BlackBerry device and the MDS or data/ application server.

NOTE: Before configuring the MDS, determine which DoD servers, Intranet sites, and Internet sites will be accessible to device users. Also, determine which application servers are allowed to push content to BlackBerry devices and from which web and application servers users are allowed to pull content.

3.3.1 Configuring BlackBerry Authentication To Web Servers

BlackBerry supports two methods for authentication to web servers: BlackBerry devices authenticate directly with web servers (after user enters their authentication credentials) or the BlackBerry MDS Connection Service authenticates with web servers on behalf of the BlackBerry device. Since the BlackBerry MDS Connection Service does not support either NTLMv2 or CAC authentication, the MDS must be configured for direct BlackBerry device authentication to web services as follows:

1. In the BlackBerry Manager, select a BlackBerry MDS Connection service in the left pane
2. On the **Connection Service** tab, select **Edit Properties**
3. Select **HTTP**
4. Select **Support HTTP Authentication**
5. In the drop-down list, select **False**

3.3.2 Data Encryption

When data is sent between the MDS and the BlackBerry device it is encrypted using the same data encryption processes that are used to encrypt wireless email between the BES and the BlackBerry device. In addition, SSL or TLS security encryption can be enabled for those application servers that require secure connections.

3.3.3 MDS Properties

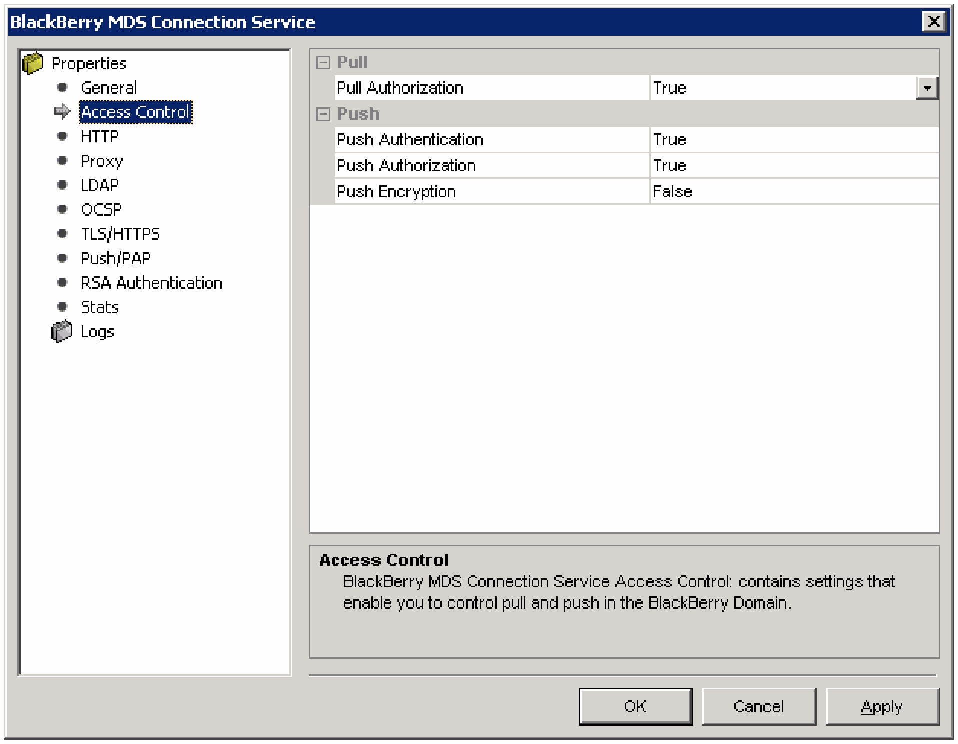
The following tables and figures show security related MDS properties and ***required*** or **optional** configuration settings for those properties.

Access Control Properties

If MDS Push or Pull connection servers and applications are set up, configure the access control properties as follows:

Local Access Control Properties		
MDS Property	**Setting**	
	Required	**Optional**
Pull Access Control: Authorization Enabled	TRUE	
Push Access Control: Authentication Enabled	TRUE	
Push Access Control: Authorization Enabled	TRUE	
Push Access Control: Encryption Enabled		TRUE

Table 3-1. Local Access Control Properties



Pull
Pull Authorization True
Push
Push Authentication True
Push Authorization True
Push Encryption False

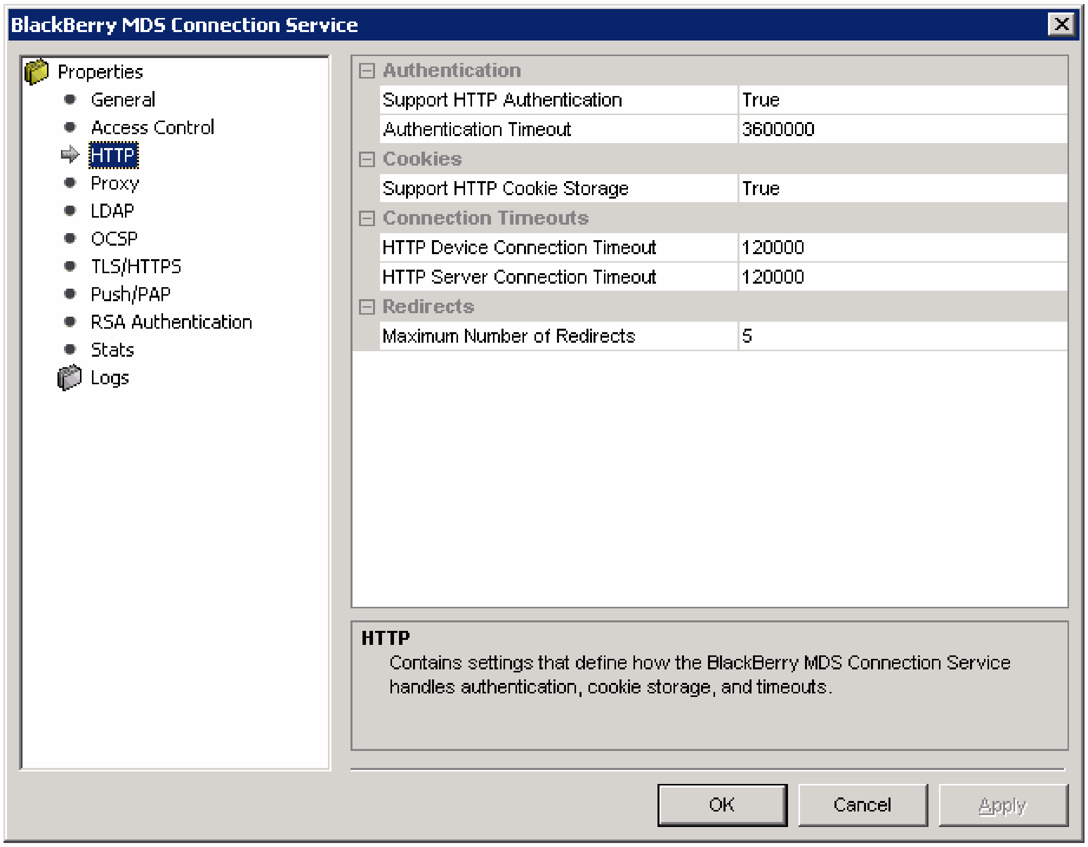
Access Control
BlackBerry MDS Connection Service Access Control: contains settings that enable you to control pull and push in the BlackBerry Domain.

Figure 3-6. Screen Shot – Configuring Local Access Control

HTTP Properties

HTTP Properties		
MDS Property	Setting	
	Required	Optional
Support HTTP Authentication		TRUE
Authentication Timeout		3600000
Support HTTP Cookie storage		FALSE
HTTP handheld connection timeout (milliseconds)		120000
HTTP server connection timeout (milliseconds)		120000
Maximum number of redirects		5

Table 3-2. HTTP Properties



Authentication

Support HTTP Authentication	True
Authentication Timeout	3600000

Cookies

Support HTTP Cookie Storage	True

Connection Timeouts

HTTP Device Connection Timeout	120000
HTTP Server Connection Timeout	120000

Redirects

Maximum Number of Redirects	5

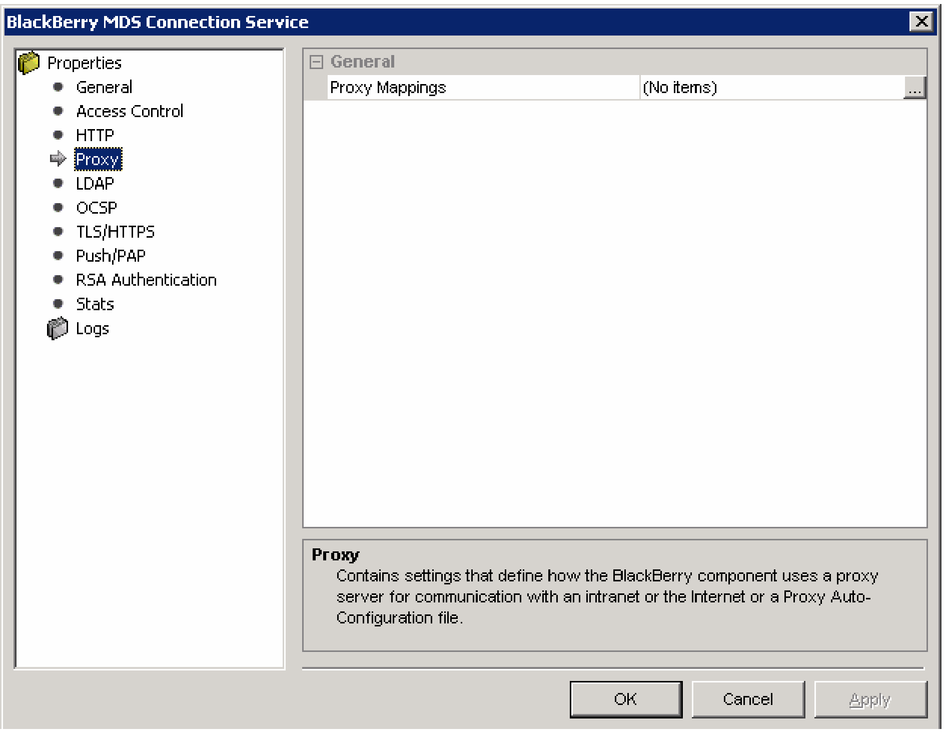
HTTP
Contains settings that define how the BlackBerry MDS Connection Service handles authentication, cookie storage, and timeouts.

Figure 3-7. Screen Shot – Configuring HTTP

Proxy Properties

Proxy Properties		
MDS Property	Setting	
	Required	Optional
Proxy Mappings		Specify required mappings

Table 3-3. Proxy Properties



Proxy Mappings (No items)

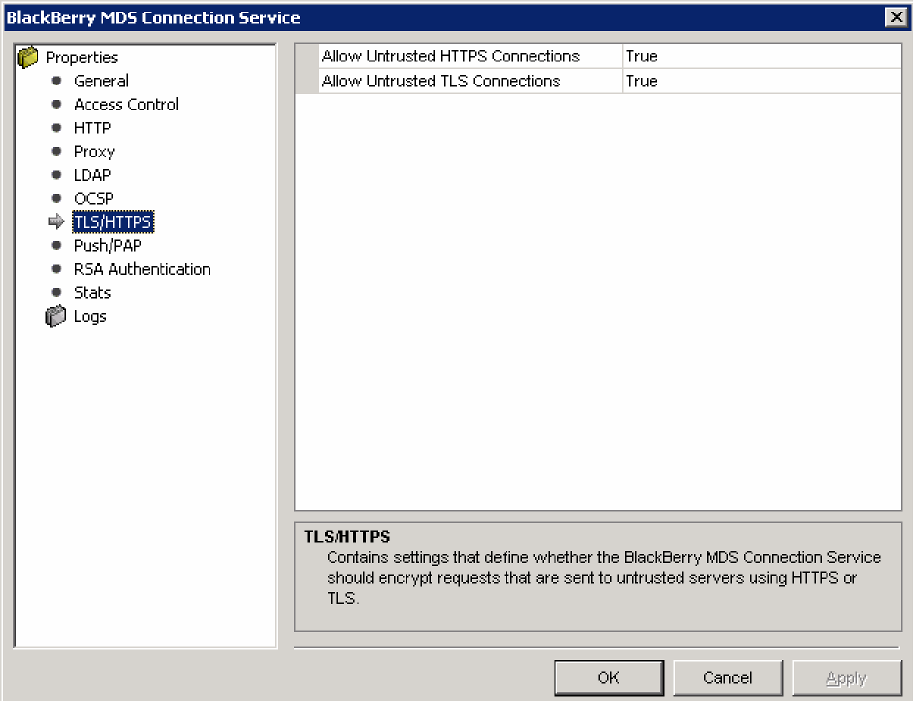
Proxy
Contains settings that define how the BlackBerry component uses a proxy server for communication with an intranet or the Internet or a Proxy Auto-Configuration file.

Figure 3-8. Screen Shot – Configuring Proxy Properties

TLS/HTTPS Properties

TLS and HTTPS Properties		
MDS Property	Setting	
	Required	Optional
Allow Untrusted HTTPS Connections		FALSE
Allow Untrusted TLS Connections		FALSE

Table 3-4. TLS and HTTPS Properties



BlackBerry MDS Connection Service

Allow Untrusted HTTPS Connections	True
Allow Untrusted TLS Connections	True

TLS/HTTPS
Contains settings that define whether the BlackBerry MDS Connection Service should encrypt requests that are sent to untrusted servers using HTTPS or TLS.

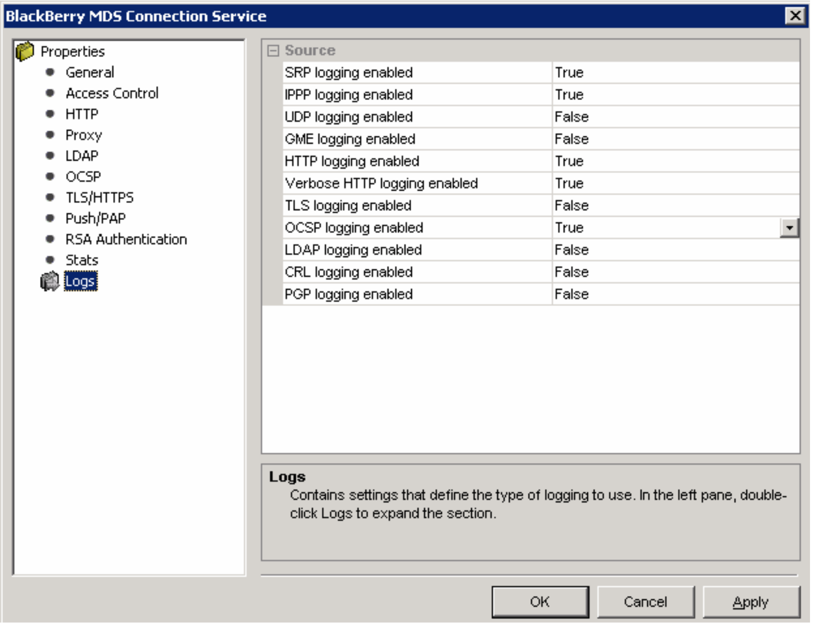
Figure 3-9. Screen Shot – Configuring TLS and HTTPS Properties

Logs Properties

Logs Properties		
MDS Property	Setting	
	Required	Optional
Logging Level Detail		HTTP logs, TLS Logs

Table 3-5. Log Properties

NOTE: A sound best practice is for each site to keep logs for 30 days. Logs can be kept 7 days or less on the BES server and then archived offline.



Source	
SRP logging enabled	True
IPPP logging enabled	True
UDP logging enabled	False
GME logging enabled	False
HTTP logging enabled	True
Verbose HTTP logging enabled	True
TLS logging enabled	False
OCSP logging enabled	True
LDAP logging enabled	False
CRL logging enabled	False
PGP logging enabled	False

Logs
Contains settings that define the type of logging to use. In the left pane, double-click Logs to expand the section.

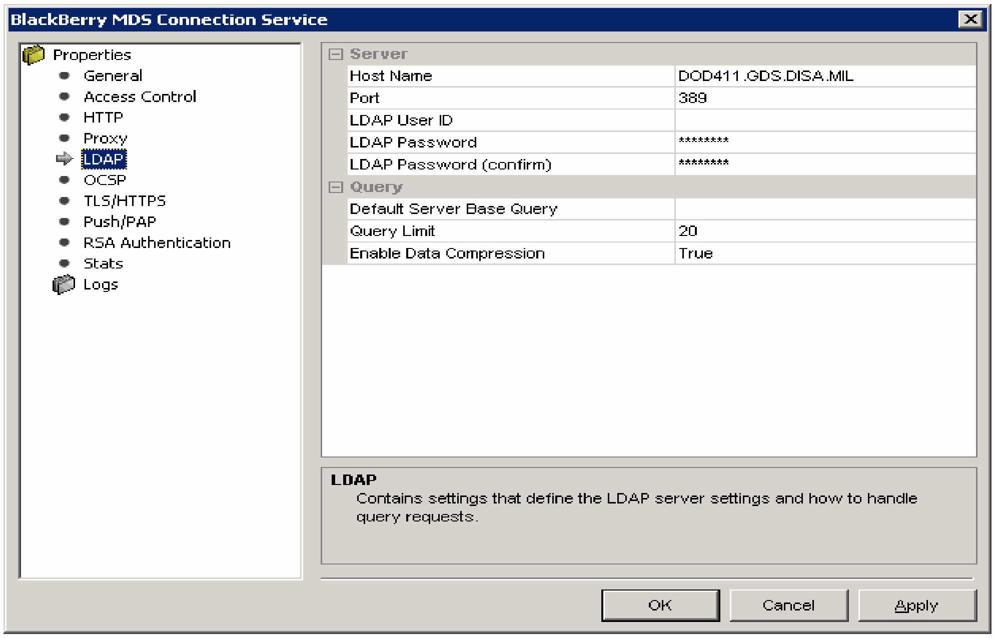
Figure 3-10. Screen Shot – Configuring Logs

CRL Properties

The Certificate Revocation List (CRL) should not be configured on a DoD BES. The BES is limited to configuration of only one CRL connection. The current DoD PKI has over 20 CRL locations. OCSP must be configured instead.

LDAP Properties

Only one LDAP can be defined at the BES level. See Figure 3.11. Additional connections to different LDAPs would be configured through the BlackBerry Desktop Manager.



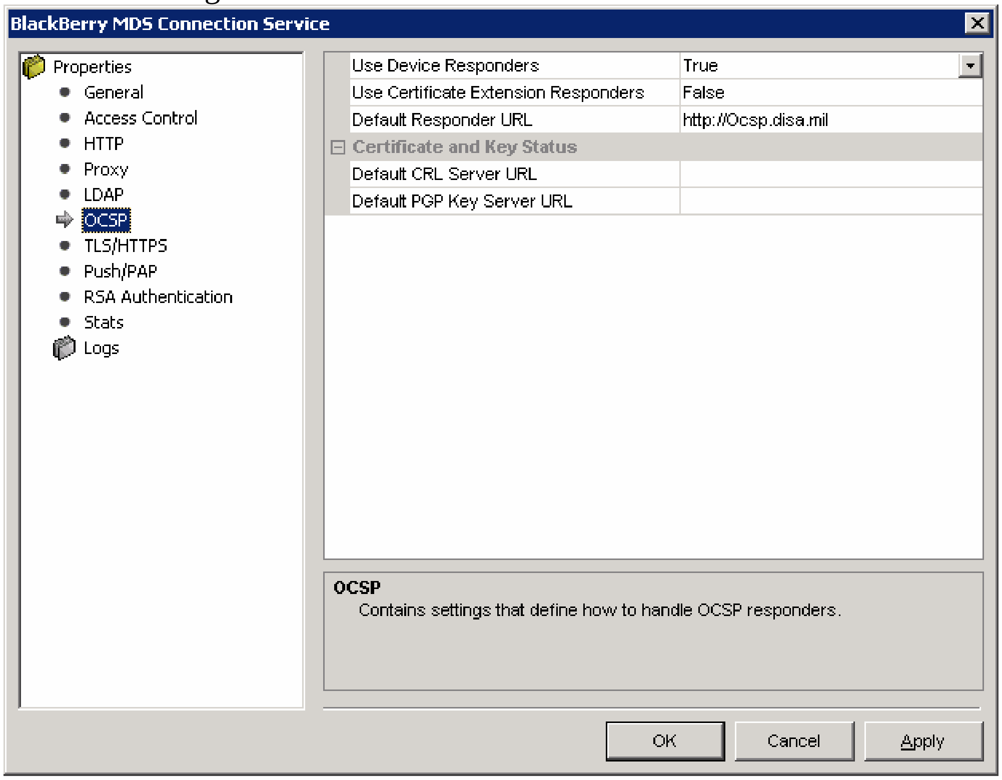
Server	
Host Name	DOD411.GDS.DISA.MIL
Port	389
LDAP User ID	
LDAP Password	********
LDAP Password (confirm)	********
Query	
Default Server Base Query	
Query Limit	20
Enable Data Compression	True

LDAP
Contains settings that define the LDAP server settings and how to handle query requests.

Figure 3-11. Screen Shot – LDAP Configuration

OCSP Properties

OCSP provides certificate validation services for all DoD PKI issued certificates in one location. Configure as shown in Figure 3.12.



Use Device Responders	True
Use Certificate Extension Responders	False
Default Responder URL	http://Ocsp.disa.mil
⊟ Certificate and Key Status	
Default CRL Server URL	
Default PGP Key Server URL	

OCSP
Contains settings that define how to handle OCSP responders.

Figure 3-12. Screen Shot – OCSP Configuration

3.4 S/MIME Configuration

References:

– BlackBerry Enterprise Server for Microsoft Exchange, Version 4.1.4, System Administration Guide, page 19.
– S/MIME Support Package Security, Version 4.2, Technical Overview.
– BlackBerry Enterprise Server, All released versions (4.1.4 and earlier), Policy Reference Guide (Version 16), 10 July 2007.

The BlackBerry S/MIME Support Package (SSP), provides the capability for users to send and receive S/MIME email messages from their BlackBerry devices when S/MIME is enabled on their BES.

The following IT Policies apply to BlackBerry devices where the S/MIME Support Package is installed. Table C.1, IT Policy Rules, lists all S/MIME related ***Required*** and ***Optional*** BlackBerry IT policy settings.

S/MIME Application policy group

- S/MIME Allowed Content Ciphers
- S/MIME Force Digital Signature
- S/MIME Force Smartcard Use
- S/MIME Minimum Strong DH Key Length
- S/MIME Minimum Strong DSA Key Length
- S/MIME Minimum Strong ECC Key Length
- S/MIME Minimum Strong RSA Key Length

Security policy group

Protecting the handheld key store:

- Disable Key Store Backup
- Disable Key Store Low Security
- Minimal Encryption Keystore Security Level
- Minimal Signing Keystore Security Level

Securing certificates, certificate status and certificate revocation lists:

- Certificate Status Cache Timeout (removed in BES 4.1.2)
- Certificate Status Maximum Expiry Time
- Disable Stale Status Use
- Disable Untrusted Certificate Use
- Disable Unverified Certificate Use
- Disable Unverified CRLs
- Disable Weak Certificate Use

Enabling smart card use:

- Allow Smart Card Password Cashing
- Key Store Password Maximum Timeout
- Lock on Smart Card Removal

Enabling S/MIME messaging:

- Disable Email Normal Send
- Disable Peer-to-Peer Normal Send

Memory Cleaner policy group

- Force Memory Clean When Holstered
- Force Memory Clean When Idle
- Memory Cleaner Maximum Idle

Device Only policy group

- Allow Peer-to-Peer Messages

For S/MIME Pin-to-Pin messaging, do the following:

- Set Allow Peer-to-Peer Messages to **TRUE**

- Set Disable Peer-to-Peer Normal Send to **TRUE**
- Have recipient PIN listed in address book entry

The following recommended change should be made to the default S/MIME configuration of the BES so that “Signed” messages are not also encrypted, by default:

Change "**Enable S/MIME Encryption on Signed and Weakly Encrypted Messages**" from “**TRUE**” (default setting) to “**FALSE**.” To change the setting, go to the BlackBerry Manager, select the BES, click on the Server Configuration tab, select Edit Properties, select Messaging, and change the setting under Secure Messages.

3.5 PGP Encryption

PGP encryption should not be used on DoD BlackBerry systems. S/MIME is the standard email encryption package for DoD BlackBerry systems.

3.6 Managing Encryption Keys

References:

- BlackBerry Enterprise Server for Microsoft Exchange, Version 4.1.4, System Administration Guide, page 17.
- BlackBerry Enterprise Solution, Security Technical Overview, page 9.

Both 3DES and AES encryption are available on the BES for securing data between the BES and the BlackBerry device but AES is the preferred encryption algorithm. There are two instances where AES cannot be used: One or more BlackBerry handheld devices in the enterprise are running a version of BlackBerry Handheld Software version 3.7 or below or the BlackBerry device is a C++ handheld.

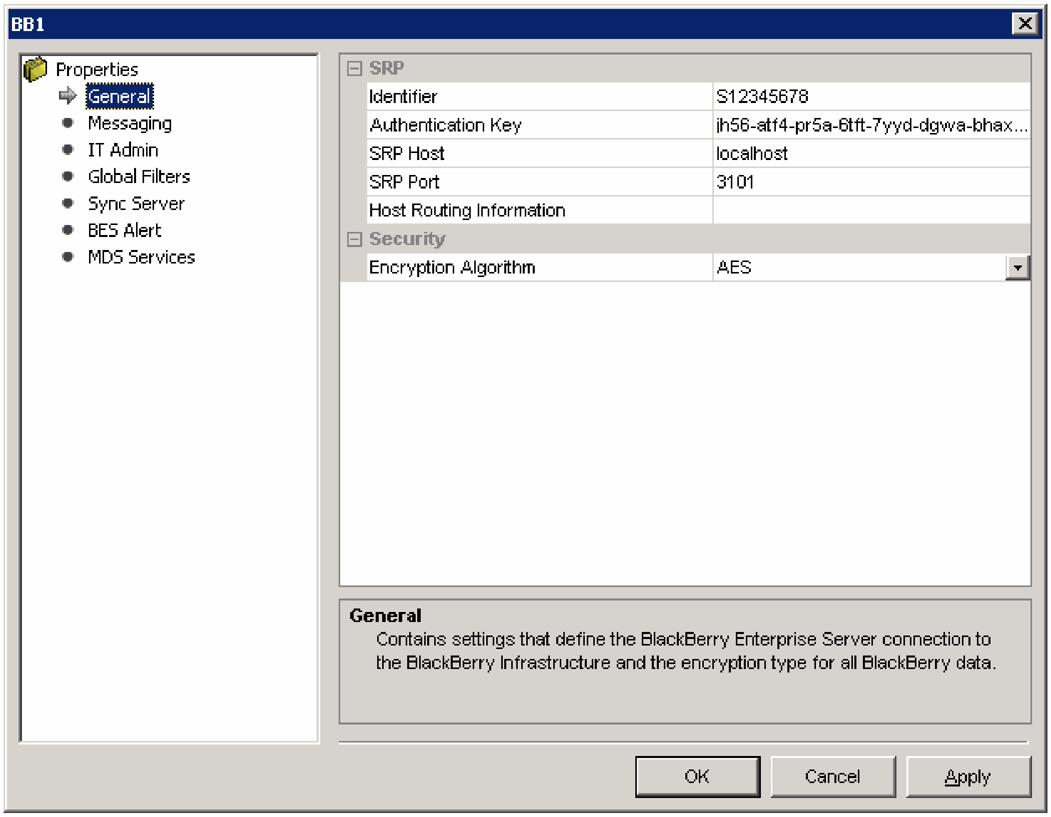
Select Master Key Algorithm

Select the Master Key on the BES as follows:

1. In the BlackBerry Manager, right-click a server and select a **BlackBerry Enterprise Server** in left pane
2. In the right pane, select **Edit Properties**
3. Select **General** tab**.**
4. **In the Security section, click Encryption types:**

AES	for AES encryption (Cannot be used in an environment where one or more BlackBerry handheld devices in the enterprise are running a version of BlackBerry Handheld Software version 3.7 or below or the BlackBerry device is a C++ handheld)
Triple DES	for 3DES encryption

Triple DES & AES for a transitional environment where both BlackBerry Handheld Software version 4.0 and earlier versions are being used (defaults to 3DES when earlier version systems are still being used)



SRP	
Identifier	S12345678
Authentication Key	ih56-atf4-pr5a-6tft-7yyd-dgwa-bhax...
SRP Host	localhost
SRP Port	3101
Host Routing Information	
Security	
Encryption Algorithm	AES

General
Contains settings that define the BlackBerry Enterprise Server connection to the BlackBerry Infrastructure and the encryption type for all BlackBerry data.

Figure 3-13. Screen Shot – Selecting Master Key Algorithm

The following IT Policies apply to the selection and protection of Master Keys. Table C.1, IT Policy Rules, lists all related ***Required*** and ***Optional*** BlackBerry IT policy settings.

Security policy group

- Disable 3DES Transport Crypto
- Force Content Protection of Master Keys

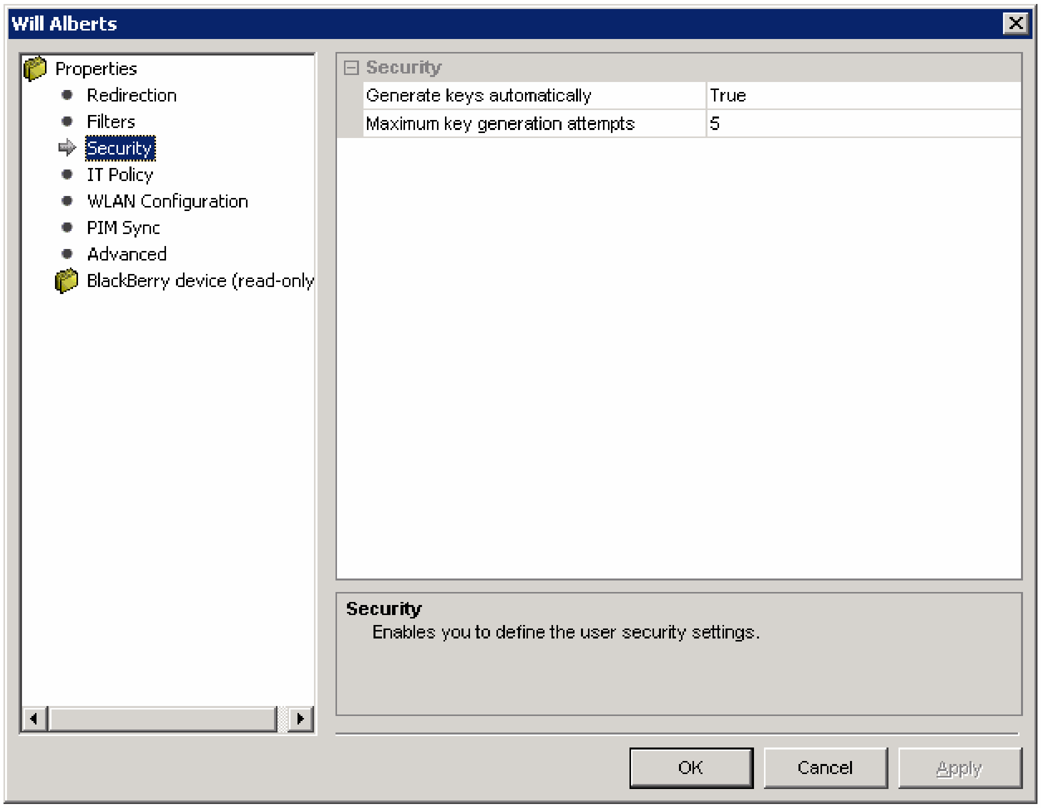
Master Key Generation

The BES can be configured to generate a new Master Key either automatically or manually. The required configuration is to generate new keys automatically. The Master Key will be marked as an “Old Key” after 30 days (when automatic key generation is selected). The first time the device is connected to the desktop after the 30th day the BES will automatically generate a new key. Local policies should include requiring the device to be cradled once every 30 days.

- *(WIR1260: CAT I) The IAO will ensure automatic Master Key generation is configured on the BES.*

Steps to configure Master Key generation:

1. In the BlackBerry Manager, select a server
2. In the **User Name** list, select a user name, right click and then click on **Properties** (or select user name and double click on it)**.**
3. On the Security tab, select the Generate keys automatically option.
4. Choose Maximum key generation attempts (recommend 5 or less).
5. Select **OK**.



Security	
Generate keys automatically	True
Maximum key generation attempts	5

Security
Enables you to define the user security settings.

Figure 3-14. Screen Shot – Generating Master Key

3.7 Maintenance Configuration

3.7.1 Logging

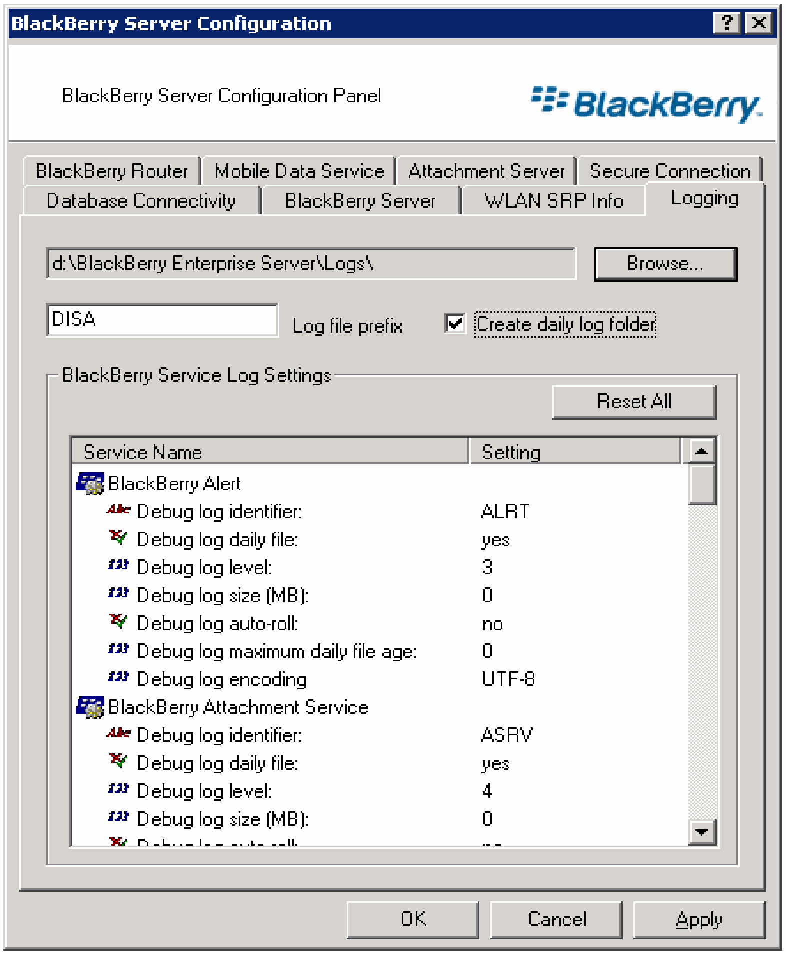
Reference:

– BlackBerry Enterprise Server for Microsoft Exchange, Version 4.1.4, System Administration Guide, page 119.

BlackBerry Enterprise Server event logs are a key tool for monitoring BlackBerry system security events and the BES should be configured to log system events. Logs can be configured to record Global events (all log files on the BES) or at the component/service level. BES components include (Router, Dispatcher, Messaging Agent, Controller, Attachment Service, Synchronization Service, Mobile Data Service, Policy Service, Database).

Steps to configure global BES logs:

1. Start > Programs > BlackBerry Enterprise Server > BlackBerry Server Configuration
2. Select Logging tab
3. Modify desired parameters:
    - **Log Root Location** Type the desired root folder for logs, or click browse
    - **Log file prefix** Type the desired custom prefix to add to all log file names
    - **Create daily log folder** Type **Yes** if daily log files are desired
4. Select **OK**



d:\BlackBerry Enterprise Server\Logs\

DISA Log file prefix

☑ Create daily log folder

BlackBerry Service Log Settings

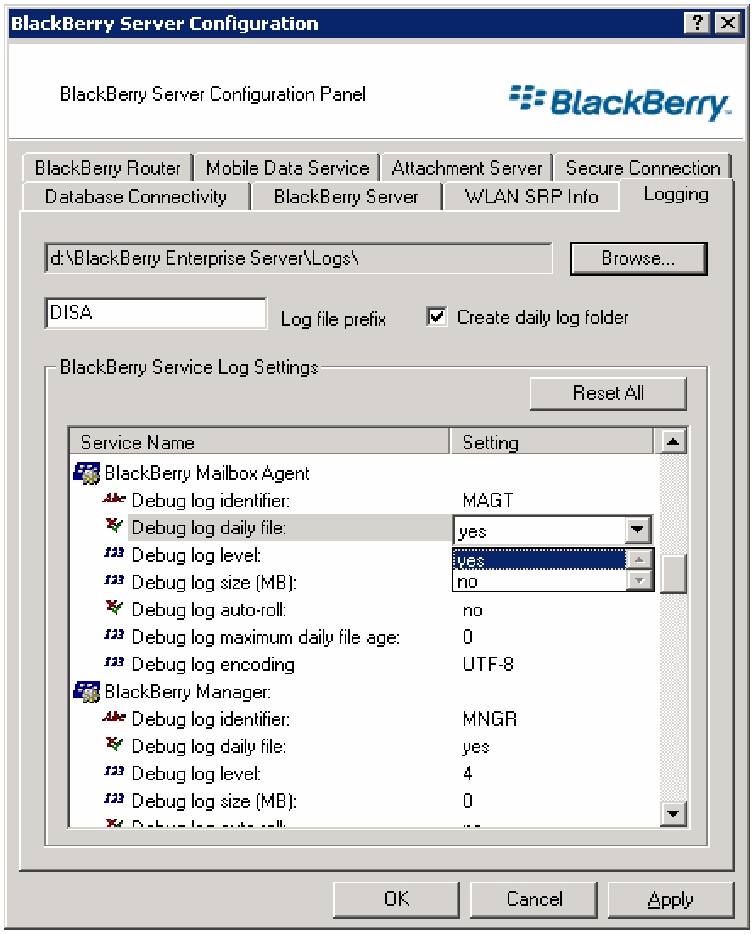
Service Name	Setting
BlackBerry Alert	
Debug log identifier:	ALRT
Debug log daily file:	yes
Debug log level:	3
Debug log size (MB):	0
Debug log auto-roll:	no
Debug log maximum daily file age:	0
Debug log encoding	UTF-8
BlackBerry Attachment Service	
Debug log identifier:	ASRV
Debug log daily file:	yes
Debug log level:	4
Debug log size (MB):	0

Figure 3-15. Screen Shot – Configuring Global BES Logs

Steps to configure component BES logs:

1. Start > Programs > BlackBerry Enterprise Server > BlackBerry Server Configuration
2. Select Logging tab, then select a Server component or service
3. Modify desired parameters:
    - **Debug log identifier** Type new default four letter identifier for component
    - **Debug daily log file** Type **Yes** if daily log files are desired

- **Debug log level** Select level of logging
- **Debug log size** Select value of maximum log size
- **Debug log auto-roll** Select if new log file is created when component is restarted or the maximum log size is reached.
- **Debug log maximum** Select maximum log age in days
- **Daily file age** Select maximum log age in days. Select at least one day longer than period logs are moved to offline storage (e.g., select 8 days if standard procedures is to move Daily logs on BES to offline storage every 7 days).



d:\BlackBerry Enterprise Server\Logs\

DISA Log file prefix

☑ Create daily log folder

BlackBerry Service Log Settings

Service Name	Setting
BlackBerry Mailbox Agent	
Debug log identifier:	MAGT
Debug log daily file:	yes
Debug log level:	yes no
Debug log size (MB):	
Debug log auto-roll:	no
Debug log maximum daily file age:	0
Debug log encoding	UTF-8
BlackBerry Manager:	
Debug log identifier:	MNGR
Debug log daily file:	yes
Debug log level:	4
Debug log size (MB):	0

Figure 3-16. Screen Shot – Configuring component BES Logs

4. Select **OK**
5. Restart the component

NOTE: RIM recommends that 30 days of daily log files be maintained for each component or service for system troubleshooting purposes. No more than seven days of logs should be maintained on the same server that the BES is installed on, therefore the BES administrator should move logs to offline storage every 7 days or less.

3.7.2 BES Alert Settings

Reference:

- User Guide, BlackBerry Enterprise Server Alert Tool

The BES Alert Tool monitors the Microsoft Windows Event log and sends defined users email messages containing alert notifications when certain events are recorded in the Event log. Types of events monitored include critical, errors, warnings, and information.

- **Critical** messages are generated by events that affect the operation of the BES.
- **Error** messages are generated by events that affect email redirection for all BlackBerry users.
- **Warning** messages are generated by events that affect email redirection for one or more (but not all) BlackBerry users.
- **Informational** events are generated by any action performed by the BES.

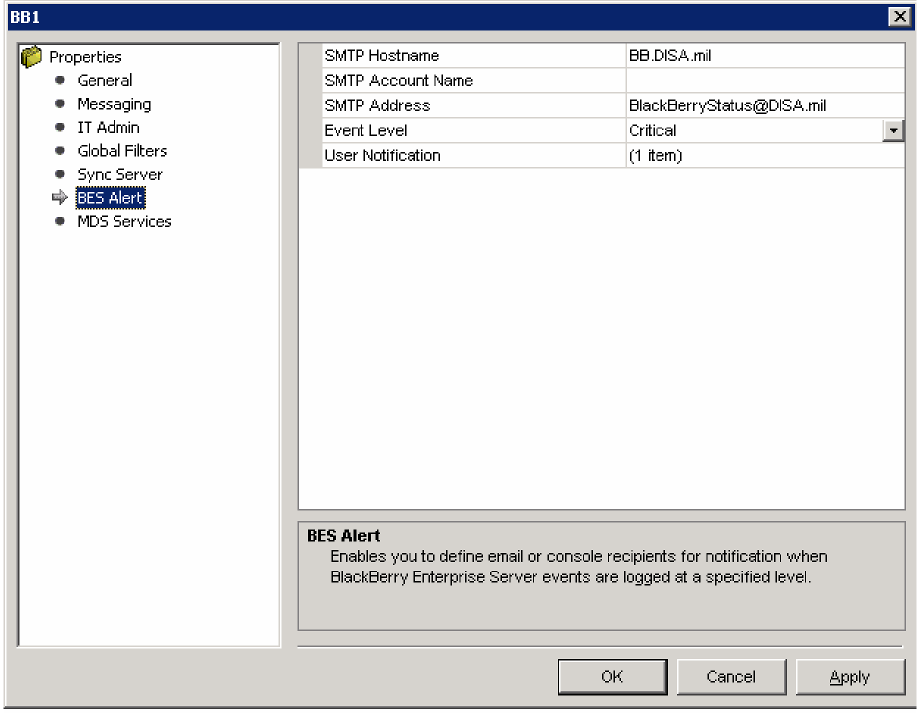
When selecting **Critical**, includes **Critical** messages only.
When selecting **Error**, includes **Critical** and **Error** messages.
When selecting **Warning**, includes **Critical**, **Error**, and **Warning** messages.
When selecting **Informational**, includes **Critical**, **Error**, **Warning**, and **Informational** messages.

BES Alert Setting		
Configuration or Action	**Setting**	
	Required	**Optional**
BES Alert		**Critical, Error** or **Warning**

Table 3-6. BES Alert Setting

To configure the BES Alert, follow the instructions under **Set the default event monitoring level** on page 2 of the *User Guide, BlackBerry Enterprise Server Alert Tool.*

To define a BES Alert message recipient, follow the instructions under **Define a notification recipient** on page 2 of the *User Guide, BlackBerry Enterprise Server Alert Tool.*



SMTP Hostname	BB.DISA.mil
SMTP Account Name	
SMTP Address	BlackBerryStatus@DISA.mil
Event Level	Critical
User Notification	(1 item)

BES Alert
Enables you to define email or console recipients for notification when BlackBerry Enterprise Server events are logged at a specified level.

Figure 3-17. Screen Shot – Configuring BESAlert

3.7.3 System Backup

References:

- BlackBerry Enterprise Server for Microsoft Exchange, Version 4.1.4, System Administration Guide, page 79.

Full system backups should be performed regularly on BES data to protect the BlackBerry system against system data loss or unavailability. The following BES data should be backed up:

- BES registry settings
- Log files
- Attachment service executables and supporting files
- Microsoft Exchange user mailbox information and hidden BlackBerry files

The BlackBerry Backup tool is used to manage data backup and recovery. Procedures for using the tool are found in Appendix D of the BlackBerry Enterprise Server for Microsoft Exchange, Version 4.0, Maintenance Guide.

3.8 Control of Third-Party Applications

References:

- BlackBerry Enterprise Server for Microsoft Exchange, Version 4.1.4, System Administration Guide, page 41.
- BlackBerry Enterprise Solution, Security Technical Overview, page 7.

- BlackBerry Enterprise Server, All released versions (4.1.4 and earlier), Policy Reference Guide (Version 16).

- *(WIR1180: CAT I) The IAO will ensure wireless push email device users can not install or remove applications and/or software on their handheld device, unless the process is directed by the IAO and under the supervision of an authorized system administrator. Enforcement must be via system security policy.*

- *(WIR1190: CAT I) The IAO will ensure Onset Technologies Metamessage software is not installed on BlackBerry devices or on the BES.*

RIM handheld software and third-party applications installed on the BlackBerry device should be controlled via IT Policy rules and by creating application control policies. IT Policy rules are used to set broad rules that affect all third-party applications (e.g. allow or disallow downloads of third-party applications) while application control policies are used to control specific applications.

The following IT Policies apply to BlackBerry devices where third-party applications are installed. Table C.1, IT Policy Rules, lists all third-party application related ***Required*** and ***Optional*** BlackBerry IT policy settings.

Desktop policy group

- Desktop Allow Desktop Add-Ins

Security policy group

- Allow Third Party Apps to Use Serial Port
- Allow Third Party Apps to Use Persistent Store
- Disallow Third Party Application Downloads

BES System Administrators should define application control policies to control each third-party application used on BlackBerry devices in their BlackBerry domain. If no third party applications are required, set up an application control policy on the BES to block all third party applications. When third party applications are required, set up an application control policy on the BES to permit only specific DAA approved applications and set up the control policy that specifies assigned permissions for the application. All application permission rules should be set to “Not Permitted” by default and set to “allowed” or “Prompt User” only if required for application operation. Only properties required by each application should be allowed.

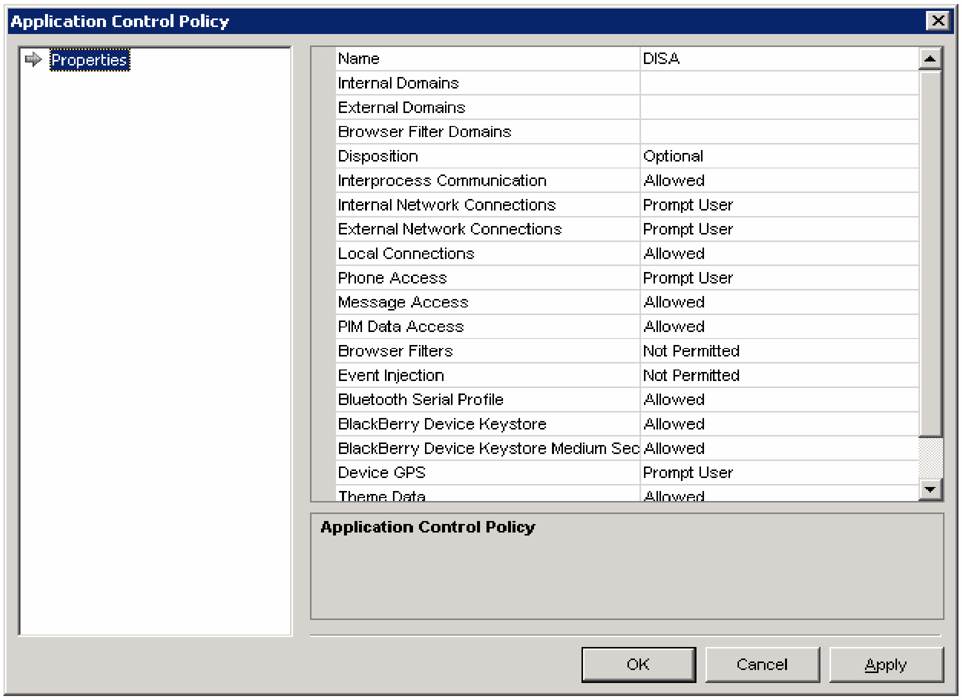
Follow the following steps for defining application control policies and assigning to applications:

1. In the BlackBerry Manager, left pane, select **BlackBerry Domain**.
2. On the **Software Configurations** tab, do the following:
3. Click **Manage Application Policies**.
4. Click **New**.
5. Type in a name for the new policy.

6. Customize the new policy.
7. On the **Software Configurations** tab, do the following:
8. In the **Configuration Name** list, click a software configuration.
9. Select **Edit Configuration**.
10. Expand the **Application Software** application tree.
11. In the **Policy** drop-down list, select an application control policy to assign to an application.

Control of Third-Party Applications		
Property	**Default Value**	**Recommended Value**
Internal Domains	NULL	Specify Domain Names
External Domains	NULL	Specify Domain Names
Browser Filter Domains	NULL	Specify Domain Names
Disposition	Optional	Specify Optional, Required, or Not Permitted for each application
Interprocess Communications	Allowed	Allowed
Internal Network Connections	Prompt User	Prompt User
External Network Connections	Prompt User	Prompt User
Local Connections	Allowed	Allowed
Phone Access	Prompt user	Prompt user
Message Access	Allowed	Allowed
PIM Data Access	Allowed	Allowed
Browser Filters	Not Permitted	Not Permitted
Event injection	Not Permitted	Not Permitted
Bluetooth Serial Profile	Allowed	Allowed
BlackBerry Device Keystore	Allowed	Allowed
BlackBerry Device Keystore Medium Security	Allowed	Allowed
Device GPS	Prompt User	Prompt User
Theme Data	Allowed	Allowed
User Authenticator API	Allowed	Allowed

Table 3-7. Control of Third-Party Applications



Name	DISA
Internal Domains	
External Domains	
Browser Filter Domains	
Disposition	Optional
Interprocess Communication	Allowed
Internal Network Connections	Prompt User
External Network Connections	Prompt User
Local Connections	Allowed
Phone Access	Prompt User
Message Access	Allowed
PIM Data Access	Allowed
Browser Filters	Not Permitted
Event Injection	Not Permitted
Bluetooth Serial Profile	Allowed
BlackBerry Device Keystore	Allowed
BlackBerry Device Keystore Medium Sec	Allowed
Device GPS	Prompt User
Theme Data	Allowed

Figure 3-18. Screen Shot – Setting Application Control Policy

3.9 Content Protection

References:

- BlackBerry Enterprise Solution, Security Technical Overview.
- BlackBerry Enterprise Server, All released versions (4.1.4 and earlier), Policy Reference Guide (Version 16).
- BlackBerry Wireless Handheld User’s Guide.

Content Protection encrypts data stored on the BlackBerry handheld device using 256-bit AES encryption. The following items are encrypted of the BlackBerry device: Email, Calendar, MemoPad, Tasks, Contacts, Auto Text, and BlackBerry Browser.

Content Protection can be enabled either by an IT Policy configuration setting or by selecting the Content Protection option on the BlackBerry device. When implemented, Content Protection should be enabled via an IT Policy configuration setting.

NOTE**:** When Content Protection is enabled, the BES system administrator *cannot* remotely unlock a BlackBerry device and remotely reset the device password, which may be a critical mission requirement at some DoD facilities. RIM will release an update to the BES in late 2007 to provide remote device unlock / password reset when Content Protection is enabled.

The following IT Policy applies to Content Protection on BlackBerry devices. Table C.1, IT Policy Rules, lists the ***Required*** and ***Optional*** BlackBerry IT policy settings.

Security policy group

- Content Protection Strength

3.10 Password Keeper Settings

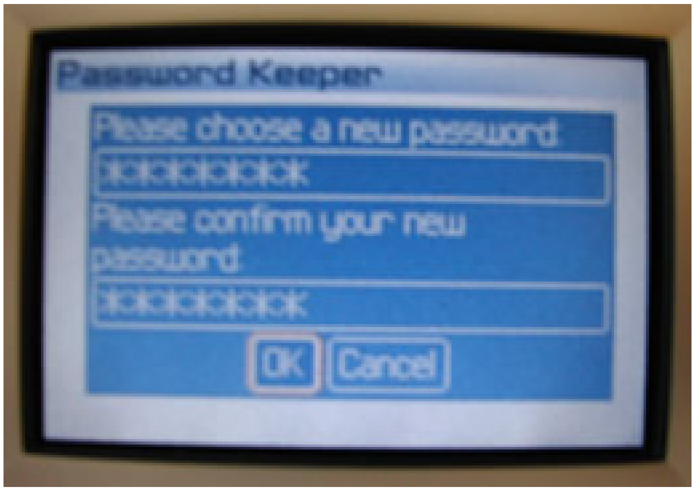
References:

- BlackBerry Enterprise Solution, Security Technical Overview, page 27.
- BlackBerry Wireless Handheld User's Guide.

Password Keeper is a third party application provided by RIM that can be installed on the BlackBerry handheld device. This application allows users to create and store passwords. The use of Password Keeper should be reviewed and approved by the local DAA. Passwords are stored using 256-bit AES encryption using the BlackBerry FIPS 140-2 certified encryption module. Passwords in the Password Keeper can be copied and pasted into other applications but the password is unencrypted while it resides in the BlackBerry handheld device clipboard.

When Password Keeper is enabled, the user must configure the application to enforce the following rules.

- Require use of a eight or more character password.
- Set the number of incorrect passwords entered before a device wipe occurs to 10 or less.
- Change the password at least every 90 days.



Password Keeper

Please choose a new password

****

Please confirm your new password:

****

Figure 3-19. Screen Shot – Setting Password Keeper password

- *(WIR1110: CAT I) The IAO will ensure that when the Password Keeper is enabled on the BlackBerry device, the DAA has reviewed and approved its use, and the application is configured to enforce the following password rules.*

  - *Require use of eight or more characters. The Password Keeper is configured to enforce this policy.*
  - *Set the number of incorrect passwords entered before a device wipe occurs to 10 or less.*

- Set local policy to require a change of password at least every 90 days.

3.11 Bluetooth Security Settings

References:

- BlackBerry Enterprise Solution, Security Technical Overview.
- BlackBerry Enterprise Server, All released versions (4.1.4 and earlier), Policy Reference Guide (Version 16).

Bluetooth wireless voice and data connections can be established between the BlackBerry handheld device and any other device with Bluetooth wireless capabilities. There are significant security issues with Bluetooth, therefore, Bluetooth should only be used as follows:

- Voice connection to a Bluetooth earbud cell phone earbud is prohibited due to Bluetooth security issues. Wired handsfree devices should be used.

- Data connections for the Bluetooth smart card reader (see section 3.12). (Only DISA tested and approved Bluetooth CAC readers may be used.)

The following IT Policy applies to Bluetooth security on BlackBerry devices. Table C.1, IT Policy Rules, lists the ***Required*** and ***Optional*** BlackBerry IT policy settings.

BlackBerry policy group

- Disable Bluetooth
- Disable Dial-Up Networking
- Disable Desktop Connectivity Content
- Disable Discoverable Mode
- Disable File transfer
- Disable Handsfree profile
- Disable Headset profile
- Disable Pairing
- Disable Serial Port Profile
- Require LED Connection Indicator
- Require Password for Enabling Bluetooth Support
- Require Password for Discoverable Mode

3.12 Bluetooth Smart Card (CAC) Reader

References:

- BlackBerry Enterprise Solution, Security Technical Overview.
- BlackBerry Enterprise Server, All released versions (4.1.4 and earlier), Policy Reference Guide (Version 16).
- BlackBerry Smart Card Reader Security Technical Overview, Release 1.5,

The Bluetooth Smart Card Reader significantly improves the ease of use of the Common Access Card (CAC) with the S/MIME Support Package. When configured properly, the Bluetooth

Smart Card Reader provides a secure wireless data connection between the smart card reader and BlackBerry device or between the smart card reader and PC. (See section 3.18 for more information on using the BlackBerry SCR with PCs.)

The following IT Policy applies to Bluetooth security for the Bluetooth Smart Card reader. Table C.1, BES IT Policy Rules, lists the required and optional BlackBerry IT policy settings.

BlackBerry policy group

- Disable Bluetooth
- Disable Desktop Connectivity Content
- Disable Discoverable Mode
- Disable Pairing
- Disable Serial Port Profile
- Require Password for Enabling Bluetooth Support
- Require Password for Discoverable Mode

BlackBerry Smart Card Reader policy group

- Force Erase All Keys on BlackBerry Disconnected Timeout
- Maximum BlackBerry Disconnected Timeout
- Maximum BlackBerry Inactivity Timeout
- Maximum Bluetooth Range
- Maximum Connection Heartbeat Period
- Maximum Long Term Timeout
- Maximum Number of BlackBerry Transactions
- Maximum Number of PC Transactions
- Maximum Number of PC Pairings
- Maximum PC Bluetooth Traffic Inactivity Timeout
- Maximum PC Disconnect Timeout
- Maximum PC Long Term Timeout
- Maximum Smart Card Not Present Timeout

***NOTE**:* Organizations should set up separate IT policy groups for users that use the Bluetooth Smart Card Reader (SCR) and for users that do not use the Bluetooth SCR.

3.13 Forcing BlackBerry Device Software Updates

A critical component of a DoD BlackBerry system security posture is ensuring all BlackBerry devices have up-to-date software and application loads on the handheld devices. Therefore BlackBerry system administrators will include rules in each IT policy users are assigned to that force upgrades to Handheld Software.

The following IT Policy applies to software updates on BlackBerry devices. Table C.1, BES IT Policy Rules, lists the ***Required*** and ***Optional*** BlackBerry IT policy settings.

Desktop Only policy group

- Force Load Count
- Force Load Message

3.14 Firewall Requirements

3.14.1 BES Architecture

References:

- Microsoft Knowledge Base article 176466, TCP ports and Microsoft Exchange: In-depth discussion http://support.microsoft.com/kb/176466
- Microsoft Knowledge Base article 179442, http://support.microsoft.com/kb/179442/en-us
- DoD Active Directory STIG

DoD policy requires isolation of the BES host server from the site's Internal LAN (also referred to as the Internal Enclave LAN). The BES and Exchange Servers must be placed on the same segment of the Internal LAN to facilitate communications. The BES also needs to communicate with other resources (e.g., email, LDAP, or OSCP servers) which may be located in various segments or security domains within the site's architecture. There are two DoD-approved BES architecture configurations: the BlackBerry DMZ Solution and the BlackBerry Host Based Firewall Solution. This section describes the architectural and firewall requirements for these two architectures.

3.14.2 BlackBerry DMZ Architecture

This architecture requires the isolation of the BES and other systems needed for BlackBerry services (e.g., email and LDAP servers) by using one or more firewalls. This architecture creates a separate security domain on the Internal LAN and is sometimes referred to as an Internal or Inner Enclave DMZ. An example of this configuration is depicted in Figure 2.1. In this architecture, the BES and Exchange servers are connected to the Internal Enclave Firewall. The cloud labeled Intranet contains the clients and other devices on the local internal network, including the site's primary Enclave Exchange Server and Active Directory Domain Controller. The firewall used must meet NIAP firewall requirements and placement must comply with the requirements of the Network Infrastructure STIG. The Exchange and LDAP servers in the BlackBerry DMZ will synchronize periodically with the Enclave Microsoft Exchange server and LDAP server.

The Firewall Administrator (FA) will configure or add the following rules to the internally facing firewall.

- Allow communications from the Intranet (internal) clients and/or servers.
- BlackBerry systems from initiating communications to Intranet clients and/or servers.
- Only sessions from Intranet clients and/or servers are authorized to initiate connections to the systems used to host BlackBerry services in the DMZ.
- The BES is only authorized to communicate with systems in the DMZ that host BlackBerry services (e.g., email server and LDAP server) and only using the authorized ports and protocols.

- The BES is only authorized to communicate outside the DMZ with specified BlackBerry services (e.g., BlackBerry SRP server, OCSP, SSL/TLS, HTTP, and LDAP).
- All outbound connections are initiated by the BlackBerry system and/or service using port 3101.
- All unneeded incoming and outgoing ports and services should be denied by default

The following table lists the default or standard ports for the needed services. Although it is possible for the site to configure TCP/UDP to use non-standard or unregistered ports for these communications, this is not recommended as it will cause unexpected results at various internal and external boundaries in the DoD Enclave.

NOTE*:* The following table is intended as a starting point and is provided by request of field sites and reviewers to facilitate firewall configuration. Use additional references from RIM, Microsoft, and DISA STIGs to tailor the firewall rule configuration to the site's specific architecture.

Service	**Protocol**	**Default Port**	**Comments**
Outgoing data connections, using SRP, to BlackBerry Infrastructure.	TCP	3101	Both the Local Gateway Firewall and the Enclave Perimeter firewall outbound rules must be configured to allow this port outbound to Internet via NIPRNet (DoD Network). This port is not allowed to traverse the Intranet boundary on the Local Gateway Firewall. (Must traverse PPS CAL boundaries 12, 10, 6, 4, and 2 when configured in compliance with the requirements of this checklist.)
Incoming and outgoing connections from the Device Manager utility installed on a PC with the handheld device attached. Used to sync the BlackBerry to the BES.	TCP	4101	Incoming and outgoing connections on the Internal Enclave (Intranet) to/from the BES (i.e., not outgoing to the Internet).
Incoming and outgoing connection to the SQL server for BlackBerry Configuration Database, MDS Service and Synchronization Service.	TCP	1433	Needed only if SQL server is located outside the DMZ.

Service	Protocol	Default Port	Comments
Outgoing connections to the enclave web server.	HTTP, HTTPS	8080, 8443	For BlackBerry browser connections to the Internet if permitted by local policy. Some sites have opted to place all application and web proxy services into an Internal Enclave DMZ network. If the DAA has approved access to these applications, then the FA will update all appropriate firewall rules to allow the BES access.
Outgoing connections to enclave application servers.	HTTP, HTTPS	8080, 8443	For approved/authorized connections to Internal Enclave application servers. Some sites have opted to place all application and web proxy services into an Internal Enclave DMZ network. If the DAA has approved access to these applications, then the FA will update all appropriate firewall rules to allow the BES access.
Outgoing connection to trusted OCSP.	HTTP	80	To obtain PKI certificate information and revocation lists.
The following are connections between the Microsoft Exchange server and the Enclave Microsoft Exchange Server. The connections are used to sync BlackBerry user account information between Exchange Servers			
RPC endpoint mapper	TCP	135	
Microsoft Exchange System Attendant service	TCP	135	
Name Service Provider Interface (NSPI)	TCP	135	
Microsoft Exchange Information Store	TCP	135	
For connection to Active Directory (AD) for NTLM authentication. This is a complex issue requiring some site-specific decisions. See references for further details.			
RPC endpoint mapper	TCP	135	
RPC (Outbound)	TCP	1024-65534	
LDAP (Outbound to master AD)	TCP/UDP	389	
LDAP (Inbound)	TCP/UDP	1024-65535	

Service	Protocol	Default Port	Comments
Internet Control Message Protocol (ICMP). Needed for Active Directory.	ICMP is directly hosted by the IP layer.	N/A	ICMP protocol must be allowed through the firewall from the clients to the domain controllers so that client applications (e.g., BES) can receive Group Policy information. ICMP is used to determine whether the link is a slow link or a fast link. ICMP is a legitimate protocol that Active Directory uses for Group Policy detection and for Maximum Transfer Unit (MTU) detection.
DNS (Outbound)	TCP/UDP	53	
DNS (Inbound)	TCP/UDP	53 and 1024-65535	
Server message block (SMB) for Netlogon (Outbound)	TCP	445	LDAP conversion, and Microsoft Distributed File System (DFS) discovery.
Kerberos	TCP/UDP	88	

Table 3-8. DMZ Firewall Architecture Ports, Protocols and Services

3.14.3 BlackBerry Host Based Firewall Architecture

In this architecture, all systems used to host BlackBerry services (e.g., email server and LDAP server) are protected behind an Internal Enclave firewall and added protection is achieved by use of a host based firewall installed on the BES server. The BES server is located directly on the Internal Enclave LAN on the same network segment as the Exchange Server.

The Local Gateway Firewall depicted in Figure 2.2 is an Internal Enclave firewall which creates a separate security domain for the site's Internal LAN. Specific firewall rules implemented on the BES firewall will vary based on the BES services used. The server will need to communicate with the LDAP server, OSCP, BlackBerry SRP, Exchange Server, SQL Server, and any other authorized resources not installed directly on the BES. Careful testing prior to deployment of the BES server will be needed to ensure proper operation while remaining compliant with DoD ports, protocols, and services policies.

In accordance with DoD policy, the administrator must configure the host based firewall policy to deny unneeded incoming and outgoing ports and services by default. Furthermore, firewall filtering rules will be documented; security alerts must be monitored; and a firewall audit log must be maintained. The firewall used for this functionality must be robust and have the capability to block both incoming and outgoing traffic.
In general, the host based firewall rules must be configured to implement the following policies:

- Internal traffic from the BES is limited to internal systems used to host the BlackBerry services (e.g., email and LDAP servers). Communications with other services, clients, and/or servers are not authorized.

- Internet traffic from the BES is limited to only specified BlackBerry services (e.g., BlackBerry SRP server, OCSP, SSL/TLS, HTTP, and LDAP). All outbound connections are initiated by the BlackBerry system and/or service.

The following table lists the default or standard ports for the needed services used for BES and BlackBerry device communications in a segmented network. Although it is possible to configure TCP/UDP to use non-standard or unregistered ports for these communications, this is not recommended as it will cause unexpected results at various internal or external boundaries in the DoD Enclave.

NOTE: The following table is intended as a starting point and is provided by request of field sites and reviewers to facilitate firewall configuration. Use additional references from RIM, Microsoft, and DISA STIGs to tailor the firewall rule configuration to the site's specific architecture.

Service	**Protocol**	**Default Port**	**Comments**
Outgoing data connections, using SRP, to BlackBerry Infrastructure.	TCP	3101	Both the Local Gateway Firewall and the Enclave Perimeter firewall outbound rules must be configured to allow this port outbound to Internet via NIPRNet (DoD Network). (Must traverse PPS CAL boundaries 12, 10, 6, 4, and 2 when configured in compliance with the requirements of this checklist.)
Incoming and outgoing connections from the Device Manager utility installed on a PC with the handheld device attached. Used to sync the BlackBerry to the BES.	TCP	4101	Incoming and outgoing connections on the Internal Enclave (Intranet) to/from the BES (i.e., not outgoing to the Internet).
Incoming and outgoing connection to the Microsoft SQL server for BlackBerry Configuration Database	TCP	1433	Needed only if SQL is on a separate server from BES.

Service	Protocol	Default Port	Comments
Outgoing connections to the Enclave web server	HTTP, HTTPS	8080, 8443	For BlackBerry browser connections to the Internet if permitted by local policy. Some sites have opted to place all application and web proxy services into an Internal Enclave DMZ network. If the DAA has approved access to these applications, then the FA will update all appropriate firewall rules to allow the BES access.
Outgoing connections to Enclave application servers	HTTP, HTTPS	8080, 8443	For approved/authorized connections to Internal Enclave application servers. Some sites have opted to place all application and web proxy services into an Internal Enclave DMZ network. If the DAA has approved access to these applications, then the FA will update all appropriate firewall rules to allow the BES access.
Outgoing connection to trusted OCSP	HTTP	80	To obtain PKI certificate information.
Connections between BES and BlackBerry Messaging Agent – Incoming data connections to the BlackBerry Dispatcher – Incoming system log connections to the BlackBerry Controller	TCP UDP	5096 4070	
Outgoing system log connections from the BlackBerry MDS Connection Service to the SNMP agent	UDP	4071	
For connections between the BES and the Enclave Microsoft Exchange Server.			
RPC endpoint mapper	TCP	135	
Microsoft Exchange System Attendant service	TCP	135	
Name Service Provider Interface (NSPI)	TCP	135	
Microsoft Exchange Information Store	TCP	135	

Service	**Protocol**	**Default Port**	**Comments**
For connection to Active Directory (AD) for NTLM authentication. This is a complex issue requiring some site-specific decisions. See references for further details.			
RPC Endpoint Mapper	TCP	135	Also mentioned in another part of the table but repeated here for clarity.
RPC (Outbound)	TCP	1024-65534	
LDAP (Outbound to AD)	TCP/UDP	389	
LDAP (Inbound)	TCP/UDP	1024-65535	
Internet Control Message Protocol (ICMP). Needed for Active Directory.	ICMP is directly hosted by the IP layer.	N/A	ICMP protocol must be allowed through the firewall from the clients to the domain controllers so that client applications (e.g., BES) can receive Group Policy information. ICMP is used to determine whether the link is a slow link or a fast link. ICMP is a legitimate protocol that Active Directory uses for Group Policy detection and for Maximum Transfer Unit (MTU) detection.
DNS (Outbound)	TCP/UDP	53	
DNS (Inbound)	TCP/UDP	53 and 1024-65535	
Server message block (SMB) for Netlogon (Outbound)	TCP	445	LDAP conversion, and Microsoft Distributed File System (DFS) discovery.
Kerberos	TCP/UDP	88	

Table 3-9. Host-Based Firewall Architecture Ports, Protocols and Services

3.15 BlackBerry IP Modem

A BlackBerry can be used as an “IP” modem or “tethered modem” to provide a wireless Internet connection for a laptop computer. In some cases, this is less expensive than buying a broadband wireless card and setting up a separate broadband wireless account. In order to use the BlackBerry IP modem feature, the following IT Policy rules must be configured as indicated:

Disable IP Modem - FALSE
Disable Radio When Cradled - 0

3.16 Disposal of BlackBerry Handhelds

Appendix B provides required BlackBerry sanitization procedures to follow prior to disposing of BlackBerry devices (e.g. donating to a charity, selling as excess inventory).

3.17 Use of "Team" BlackBerrys

Appendix G provides security requirements and procedures for setting up and using "team" BlackBerrys. A "team" BlackBerry is configured to receive email for a group email account and is shared between team members (e.g. a help desk team where the on-call team member will have the team BlackBerry).

3.18 RIM Bluetooth Smart Card Reader Connections to PCs

The RIM BlackBerry Smart Card Reader (i.e. CAC reader) is designed to connect to both the BlackBerry and to PCs with Bluetooth radios. DoDD 8100.2 requires strong security controls when Bluetooth is used in the DoD, therefore if the RIM BlackBerry Smart Card Reader is used as a PC smart card reader, the following security controls must be implemented:

- The DAA must approve the use of the RIM BlackBerry Smart Card Reader with site PCs.

- Separate BlackBerry Account Groups will be created: one for users that are authorized to use the RIM BlackBerry Smart Card Reader with their PCs and one for users that are NOT authorized to use the RIM BlackBerry Smart Card Reader with their PCs (or do not have a RIM BlackBerry Smart Card Reader). The IT Policy rule settings for the Bluetooth Smart card reader policy group will be set for each account group as indicated in Table C.1.

  (Note: Recommend 3 BlackBerry account groups be created:

  1. BlackBerry users without a smart card reader.
  2. BlackBerry users with a smart card reader, but not authorized to use the smart card reader to connect to their PC.
  3. BlackBerry users with a smart card reader and authorized to use the smart card reader to connect to their PC.)

- The BlackBerry SCR will only be used with PCs that have Windows XP SP2 installed. Using the RIM BlackBerry Smart Card Reader with Windows Vista is not approved since DoD testing of the Vista Bluetooth stack has not been completed and configuration procedures for Vista have not been developed. Blackberry users with Vista on their PCs must be put in the BlackBerry users group not authorized to use the BlackBerry SCR with their PCs.

- Bluetooth radios must be disabled in all PCs where users do not have a RIM BlackBerry Smart Card Reader or the use of the RIM BlackBerry Smart Card Reader has not been approved by the DAA. Bluetooth radios will be disabled either by removing the radio from the PC and/or by Windows group policy.

- Only Bluetooth Class 2 or 3 radios must be used by the PC. Class 1 (100 mW) Bluetooth radios are not allowed. Also, Bluetooth controllers on the PC must support 128-bit Bluetooth encryption.

  Note: Many vendors do not disclose the class of the Bluetooth radio in their product data or specification sheets, therefore the vendor's technical support office may need to be contacted for this information. For laptops, look under the specification section of the Bluetooth Network Interface Card manual, which can be downloaded from the laptop vendor's web site or the Bluetooth dongle vendor's web site.

- Only RIM BlackBerry Smart Card Reader operating system version 1.5.1 (platform 1.5.0.81) or later will be installed on the smart card reader and BlackBerry Smart Card reader software application version 4.2.0.88 or later will be installed on the Bluetooth enabled PC. (Note, RIM indicates 4.2.0.88 refers to the reader driver version and 1.5.0.81 refers to the reader operating system version.) In addition, the RIM Bluetooth Lockdown tool will be installed and enabled (check **Restrict Bluetooth Functionality**) during installation of the BlackBerry Smart Card Reader Software. Installation should be performed by the authorized BlackBerry system administrator.

- The site Windows group security policy will set to restrict the capability of the PC user to disable, remove, or change the configuration of the RIM Bluetooth Lockdown tool.

- Users with administrative account rights to their PC must be trained to never disable the RIM Bluetooth Lockdown tool on their PC. PC Administrators should NEVER change any Bluetooth settings followings implementation of Bluetooth lockdown.

Note: The RIM Bluetooth smart card reader will not operate unless the Bluetooth radio in the PC uses the Microsoft Windows Bluetooth stack. Some Bluetooth USB adapters do not use the Windows Bluetooth stack and install an alternate Bluetooth stack when the adapter drivers are installed on the PC (or provide the option to install an alternate Bluetooth stack). Additional information can be found at the following we site: http://hellalame.com/bluetooth.htm.

NOTE: A known bug exists in RIM SCR driver, Platform 1.5.0.81 and app 4.2.0.88, dated 13 August 2007. When Bluetooth encryption is enabled (a required BES IT Policy rule setting), the BlackBerry SCR may not connect to the BlackBerry. As of 13 November 2007 RIM has not announced a date that an update to the SCR driver will be released. Until a BlackBerry SCR update is released, it is recommended that SCR driver version 1.5 be used.

3.19 Using Software Certificates

DoD PKI issued digital certificates are used to digitally sign and encrypt email. When using PKI digital certificates with a handheld device (e.g. BlackBerry, Windows Mobile Smartphone), a user's digital certificates can be stored either on the handheld (soft certs) or on their Common Access Card (CAC) (hard certs). Software certificates are defined as any PKI certificate that does not require the presence of a common access card, smart card, or alternate hardware token for the certificate to be used for digital signature or encryption operations.

Software certificate use by end users must be approved by the Component DAA, and remain in use only for the minimum time necessary to comply with the hardware token requirement. Approval of software certificate usage by the DAA can be for general use cases for groups of individuals or organizations to preclude DAA's approving individual end user instances of software certificate usage.

The current JTF-GNO position is that they prefer the usage of CAC for S/MIME requirements for BlackBerry and Windows Mobile handheld devices, but the use of software certificates is not precluded.

This page is intentionally blank.

APPENDIX A. REFERENCES

A.1 Primary References

BlackBerry Enterprise Server for Microsoft Exchange, Version 4.1.4, System Administration Guide,
http://www.BlackBerry.com/knowledgecenterpublic/livelink.exe/fetch/2000/8067/645045/7963/customview.html?func=ll&objId=7963&objAction=browse&sort=name44

Placing the BlackBerry Enterprise Solution in a segmented network, BlackBerry Enterprise server version 4.0 and later,
http://na.BlackBerry.com/eng/ataglance/security/

BlackBerry Smart Card Reader, Version 1.5 Service Pack 1, Security Technical Overview,
http://www.blackberry.com/knowledgecenterpublic/livelink.exe?func=ll&objId=1371440&objAction=browse&sort=name44

Restricting Bluetooth technology on Bluetooth enabled computers, 2007 RIM document,
http://www.blackberry.com/knowledgecenterpublic/livelink.exe/fetch/2000/8067/645045/7963/1181994/1181835/1371440/Restricting_Bluetooth_technology_on_Bluetooth_enabled_computers_-_BlackBerry_Smart_Card_Reader_Technical_Overview.pdf?nodeid=1371396&vernum=0

RIM Document KB13504, New features in BlackBerry Smart Card Reader 1.5.1, Aug 13, 2007,
http://www.BlackBerry.com/btsc/search.do?cmd=displayKC&docType=kc&externalId=KB13504&sliceId=SAL_Public&dialogID=23986423&stateId=0%200%2023984672

BlackBerry Smart Card Reader Security Technical Overview, Release 1.5,
http://na.BlackBerry.com/eng/ataglance/security/products/smartcardreader/

BlackBerry with the S/MIME Support Package, White Paper, Version 4.2
http://na.BlackBerry.com/eng/ataglance/security/products/smime.jsp

BlackBerry Enterprise Server, All released versions (4.1.4 and earlier), Policy Reference Guide (Version 16), 10 July 2007.
http://na.BlackBerry.com/eng/ataglance/security/

BlackBerry Enterprise Solution, Security Technical Overview, for BlackBerry Enterprise Server Version 4.1 Service Pack 4 and BlackBerry Device Software Version 4.2 Service Pack 2,
http://na.BlackBerry.com/eng/ataglance/security/

A.2 Additional References

Preliminary Security Evaluation of RIM’s BlackBerry-to-Smart Card Reader Bluetooth Interface, Headquarters Army Materiel Command (AMC) Report, 7 April 2006 (FOUO).

Technical Evaluation of RIM’s Smart Card Reader, BlackBerry Bluetooth Support, and Bluetooth Headsets; NSA; I332-013R-2006 ; 12 May 2006 (SECRET).

This page is intentionally blank.

APPENDIX B. BLACKBERRY DISPOSAL PROCEDURES

Detailed Procedures for Sanitizing DoD BlackBerry Devices Prior to Disposal[1]

1. Load the default or generic BlackBerry IT Policy on the BlackBerry.
    a. Wipe the old IT Policy from the registry on the desktop by performing the **Desktop Registry Clear Procedure.**
    b. Obtain a generic policy.bin file (One example can be found here: (http://voicecareaustralia.com.au/dumpster/BlackBerry/files/policy.bin).
    c. Place the downloaded file in the following directory on the desktop computer used to load software on the BlackBerry (computer where **BlackBerry Desktop Manager** is loaded): **C:\Program Files\Research In Motion\BlackBerry.**
    d. Sync the BlackBerry device with the Desktop Manager – the existing IT Policy will now be erased from the device.
2. Obtain and install Javaloader.exe on the computer where **BlackBerry Desktop Manager** is loaded (can be found at http://www.BlackBerry.com/developers/downloads/jde/index.shtml - installs as part of the JDE – javaloader.exe is a DOS application).
3. Wipe contents of the BlackBerry device:
    a. Connect BlackBerry device to USB cable/computer and run "**javaloader –usb wipe**" command from DOS prompt. This will completely erase the contents of the BlackBerry device.
    b. Allow device to reset (will not be functional at this point).

Desktop Registry Clear Procedure

1. Go to Start button, select run, then type **regedit**
2. Find the following registry key: **HKEY_Current_Users\Software\Research In Motion\BlackBerry\PolicyManager**
3. **Right-click** the above registry key and select **New ->String Value**
4. **Type** the word **Path** in the value field
5. **Double-click** the **Path key** from above and enter the following in the Value data field: **C:\Program Files\Research In Motion\BlackBerry\policy.bin**
6. Close **regedit**

[1] This procedure assumes no classified information is on the BlackBerry. This procedure should not be used for sanitizing BlackBerrys after a Classified Message incident (CMI).

This page is intentionally blank.

APPENDIX C. BES IT POLICY RULES

NOTE: Not all IT Policy rules listed in this table are available for all versions of BES software 4.0 – 4.1.4 and Handheld software versions 4.0 – 4.3.0. See ***BlackBerry Enterprise Server All released Versions (4.1.4 and earlier), Policy Reference Guide (version 19),*** 9 August 2007 for more information.

NOTE: In the table below, "Required" IT Policy rule settings must be implemented by all DoD BlackBerry systems. "Optional" IT Policy rule settings are recommended settings and may be changed to meet mission requirements. "Default factory setting" is the default setting of a rule.

BES IT POLICY RULES

Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
		Required	Optional				
BlackBerry Messenger policy group							
Disable BlackBerry Messenger	BlackBerry Messenger		FALSE	Default factory setting			
Messenger Audit Email Address	BlackBerry Messenger		—	Default factory setting			
Messenger Audit Max Report Interval	BlackBerry Messenger		168	Default factory setting			
Messenger Audit Report Interval	BlackBerry Messenger		24	Default factory setting			
Messenger Audit UID	BlackBerry Messenger		NULL	Default factory setting			

BES IT POLICY RULES							
Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
		Required	Optional				
Bluetooth policy group							
Allow Outgoing Calls	Bluetooth	1 (Only when unlocked)			III	WIR1250	
Disable Address Book Transfer	Bluetooth	TRUE			III	WIR1140	
Disable Advanced Audio Distribution Profile	Bluetooth	TRUE			II	WIR1140	
Disable Audio/Video Remote Control Profile	Bluetooth	TRUE			II	WIR1140	
Disable Bluetooth	Bluetooth	TRUE, FALSE		Set to FALSE only if Bluetooth Smart Card Reader required (only approved devices may be used)	I	WIR1140	
Disable Desktop Connectivity	Bluetooth	TRUE		Default factory setting	III	WIR1140	
Disable Dial-Up Networking	Bluetooth	TRUE			II	WIR1140	
Disable Discoverable Mode	Bluetooth	TRUE			II	WIR1140	
Disable File Transfer	Bluetooth	TRUE			II	WIR1140	
Disable Handsfree Profile	Bluetooth	TRUE			II	WIR1140	

BES IT POLICY RULES							
Policy Rule	**Policy Group**	**Setting**		**Comments**	**Security Category Code (CAT)**	**Related Check Number**	**Check If Open Finding**
		Required	**Optional**				
Disable Headset Profile	Bluetooth	TRUE			II	WIR1140	
Disable Pairing	Bluetooth	TRUE, FALSE		Set to FALSE for users in IT policy group with Bluetooth Smart Card Reader (only approved SCRs may be used). Set to TRUE for users in IT policy group without Bluetooth SCR.	II	WIR1140	
Disable Serial Port Profile	Bluetooth	TRUE, FALSE		Set to FALSE for users in IT policy group with Bluetooth Smart Card Reader (only approved SCRs may be used). Set to TRUE for users in IT policy group without Bluetooth SCR.	II	WIR1140	
Disable Wireless Bypass	Bluetooth	TRUE		Default factory setting.	II	WIR1140	
Force CHAP Authentication Bluetooth Link	Bluetooth	FALSE		Default factory setting.	II	WIR1140	
Require Encryption	Bluetooth	TRUE			II	WIR1140	
Require LED Connection Indicator	Bluetooth	TRUE			III	WIR1140	
Require Password for Enabling Bluetooth Support	Bluetooth	FALSE		Default factory setting. Rule must be set to FALSE for SCR operation.	III	WIR1140	

BES IT POLICY RULES							
Policy Rule	**Policy Group**	**Setting**		**Comments**	**Security Category Code (CAT)**	**Related Check Number**	**Check If Open Finding**
		Required	**Optional**				
Require Password for Discoverable Mode	Bluetooth	TRUE			III	WIR1140	
Bluetooth Smart Card Reader policy group							
Disable Auto Reconnect To BlackBerry Smart Card Reader	Bluetooth Smart Card Reader	TRUE			III	WIR1150	
Force Erase All Keys on BlackBerry Disconnected Timeout	Bluetooth Smart Card Reader	FALSE		Default factory setting	III	WIR1150	
Force Erase Key on PC Standby	Bluetooth Smart Card Reader		FALSE	Default factory setting			
Maximum BlackBerry Disconnected Timeout	Bluetooth Smart Card Reader		None	Default factory setting.			
Maximum BlackBerry Bluetooth Traffic Inactivity Timeout	Bluetooth Smart Card Reader		None	Default factory setting.			

BES IT POLICY RULES							
Policy Rule	**Policy Group**	**Setting**		**Comments**	**Security Category Code (CAT)**	**Related Check Number**	**Check If Open Finding**
		Required	**Optional**				
Maximum BlackBerry Long Term Timeout	Bluetooth Smart Card Reader		None	Default factory setting.			
Maximum Bluetooth Encryption Key Regeneration Period	Bluetooth Smart Card Reader		—	Default factory setting			
Maximum Bluetooth Range	Bluetooth Smart Card Reader	2 or less 50% or less		For BES 4.0 For BES 4.1	III	WIR1150	
Maximum Connection Heart Beat Period	Bluetooth Smart Card Reader		None	Default factory setting. If set to 1, 2, or 5 seconds, battery performance decreases.			
Maximum PC Bluetooth Traffic Inactivity Timeout	Bluetooth Smart Card Reader		—	Default factory setting			
Maximum PC Disconnect Timeout	Bluetooth Smart Card Reader	0 —		Use this setting for BlackBerry Account groups where BlackBerry SCR is not allowed to connect to a PC Default factory setting . Use this setting for BlackBerry Account groups where BlackBerry SCR is allowed to connect to a PC	II	WIR1150	

BES IT POLICY RULES							
Policy Rule	**Policy Group**	**Setting**		**Comments**	**Security Category Code (CAT)**	**Related Check Number**	**Check If Open Finding**
		Required	**Optional**				
Maximum PC Long Term Timeout	Bluetooth Smart Card Reader		—	Default factory setting			
Maximum Number of BlackBerry Transactions	Bluetooth Smart Card Reader		None	Default factory setting			
Maximum Number of PC Pairings	Bluetooth Smart Card Reader	0 —		Use this setting for BlackBerry Account groups where BlackBerry SCR is not allowed to connect to a PC Default factory setting . Use this setting for BlackBerry Account groups where BlackBerry SCR is allowed to connect to a PC	II	WIR1150	
Maximum Number of PC Transactions	Bluetooth Smart Card Reader		—	Default factory setting			
Maximum Smart Card Not Present Timeout	Bluetooth Smart Card Reader		None	Default factory setting			
Browser policy group							
Allow IBS Browser	Browser	FALSE			III	WIR1240	
Disable Auto Synchronization in Browser	Browser		TRUE				
Disable Java Script in Browser	Browser		FALSE	Default factory setting			

BES IT POLICY RULES

Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
		Required	Optional				
Download Images URL	Browser		___	Default factory setting			
Download Themes URL	Browser		___	Default factory setting			
Download Tunes URL	Browser		___	Default factory setting			
MDS Browser BSM Enabled	Browser		TRUE	Default factory setting			
MDS Browser Domains	Browser		__	Default factory setting			
MDS Browser HTML Tables Enabled	Browser		FALSE	Default factory setting			
MDS Browser JavaScript Enabled	Browser		FALSE	Default factory setting			
MDS Browser Style Sheets Enabled	Browser		FALSE	Default factory setting			
MDS Browser Title	Browser		BlackBerry Browser	Default factory setting. Use default or specify a name			
MDS Browser Use Separate Icon	Browser		__	Default factory setting			
Camera policy group							
Disable Camera	Camera		TRUE				
Certificate Sync policy group							
Default CRL Server URL	Certificate Sync		__	Default factory setting			

BES IT POLICY RULES							
Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
		Required	Optional				
Default LDAP Server URL	Certificate Sync		—	Default factory setting			
Default OCSP Server URL	Certificate Sync		—	Default factory setting			
Random Source URL	Certificate Sync		—	Default factory setting			
CMIME policy group							
Allow Auto Attachment Download	CMIME Application		FALSE	Default factory setting			
Attachment Viewing	CMIME Application		TRUE	Default factory setting			
Disable Notes Native Encryption Forward And Reply	CMIME Application		TRUE	Applies to Lotus Notes only.			
Enable Wireless Message Reconciliation	CMIME Application		—	Default factory setting			
Keep Message Duration	CMIME Application		30 days	Default factory setting			
Keep Saved Message Duration	CMIME Application		90 days	Default factory setting			

BES IT POLICY RULES							
Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
		Required	Optional				
Prepend Disclaimer	CMIME Application		—	Default factory setting. If used, Prepend must not include “Sent from my BlackBerry handheld” or similar message.			
Maximum Native Attachment MFH attachment size	CMIME Application		—	Default factory setting			
Maximum Native total Attachment MFHattachment size	CMIME Application		—	Default factory setting			
Common policy group							
BlackBerry Server Version	Common		___				
Confirm On Send	Common		___	Factory default setting.			
Disable Kodiak PTT	Common		TRUE				
Disable MMS	Common	TRUE			III	WIR1220	
Disable Voice-Activated Dialing	Common		TRUE				
IT Policy Notification	Common	TRUE			III	WIR1250	

BES IT POLICY RULES							
Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
		Required	Optional				
Lock Owner Info	Common	Select 1 or 3			III	WIR0012	
Set owner Info	Common	Follow guidance in comment		DoD CIO Memorandum “Policy on Use of Department of Defense (DoD) Information Systems Standard Consent Banner and User Agreement,” dated 2 Nov 2007 requires the following message be displayed: **“I've read & consent to terms in IS user agreement.”** DoD BlackBerry sites should consider adding the following optional message: “If this BlackBerry is found, please call the following phone number xxx-xxx-xxxx.” When called, the phone number should not identify itself as a DoD organization.	III	WIR0012	
Set Owner Name	Common	Leave blank or follow guidance in comment		DoD BlackBerry sites should consider using the following message: “If this BlackBerry is found, please call the following phone number xxx-xxx-xxxx.” When called, the phone number should not identify itself as a DoD organization.	III	WIR1250	
Desktop policy group							

BES IT POLICY RULES							
Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
		Required	Optional				
Desktop Allow Desktop Add-Ins	Desktop		FALSE	TRUE may be required for some applications			
Desktop Allow Device Switch	Desktop	FALSE			II	WIR1250	
Desktop Password Cache Timeout	Desktop		10	Default factory setting			
Desktop-Only items							
Auto Backup Enabled	Desktop-Only		FALSE	Default factory setting			
Auto Backup Exclude Messages	Desktop-Only		FALSE	Default factory setting			
Auto Backup Exclude Sync	Desktop-Only		FALSE	Default factory setting			
Auto Backup Frequency	Desktop-Only		7	Default factory setting			
Auto Backup Include All	Desktop-Only		TRUE	Default factory setting			
Disable Wireless Calendar	Desktop-Only		FALSE	Default factory setting			
Do Not Save Sent Messages	Desktop-Only		FALSE				
Force Load Count	Desktop-Only	1			III	WIR1270	

BES IT POLICY RULES							
Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
		Required	Optional				
Force Load Message	Desktop-Only	Add notification message. See comments for example.		"BlackBerry device handheld software update is available. Update required by DoD policy."	III	WIR1270	
Forward Messages In Cradle	Desktop-Only		___	Default factory setting			
Message Conflict Mailbox Wins	Desktop-Only		TRUE	Default factory setting			
Message Prompt	Desktop-Only		___	Default factory setting			
Show Application Loader	Desktop-Only	FALSE			II	WIR1180	
Show Web Link	Desktop-Only		FALSE	Default factory setting			
Sync Messages Instead Of Import	Desktop-Only		TRUE	Default factory setting			
Web Link Label	Desktop-Only		Downloads	Default factory setting			
Web Link URL	Desktop-Only		___	Default factory setting			
Device IOT Application policy group							
Device Diagnostic App Disable	Device IOT Application		FALSE	Default factory setting			

BES IT POLICY RULES

Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
		Required	Optional				
Set Diagnostic Report Email Address	Device IOT Application		<blank>	Default factory setting			
Set Diagnostic Report PIN Address	Device IOT Application		<blank>	Default factory setting			
Device-Only items							
Allow BCC Recipients	Device-Only		TRUE				
Allow Peer-to-Peer Messages	Device-Only		TRUE	If Peer-to-Peer messaging allowed, than “Disable Peer-to-Peer Normal Send” must be set to “TRUE” to require S/MIME Peer-to-Peer messaging	II	WIR1220	
Allow SMS	Device-Only		FALSE	If set to TRUE, IA Awareness training must include SMS/MMS security issues.			
Default Browser Config UID	Device-Only	___		Default factory setting	III	WIR1250	
Enable Long Term Timeout	Device-Only	TRUE			III	WIR1250	
Enable WAP Config	Device-Only		FALSE	TRUE only if operational requirement			
Home Page Address	Device-Only		___	Default factory setting			
Home Page is Read-Only	Device-Only		___	Default factory setting			
Maximum Password Age	Device-Only	90 days or less, 0		Set to 0 if CAC authentication is enabled for device unlock	III	WIR1100	

BES IT POLICY RULES							
Policy Rule	**Policy Group**	**Setting**		**Comments**	**Security Category Code (CAT)**	**Related Check Number**	**Check If Open Finding**
		Required	**Optional**				
Maximum Security Timeout	Device-Only	15 or less			II	WIR1120	
Minimum Password Length	Device-Only	5 or more 6, 7, or 8		If password (PIN) device unlock used (8 or higher recommended) If CAC and password device unlock is used. Recommend Password length be set to same length as CAC PIN.	I	WIR1100	
Password Pattern Checks	Device-Only	1, 2, or 3 0, 1, 2, or 3		If password length of 5 is used. If password length of 6 or more is used	I	WIR1100	
Password Required	Device-Only	TRUE			I	WIR1100	
User Can Change Timeout	Device-Only	FALSE			II	WIR1120	
User Can Disable Password	Device-Only	FALSE		Rule not available for BlackBerry Handheld software version 4.0	I	WIR1100	
Enterprise Voice Client policy group							
Disable Enterprise Voice Client	Enterprise Voice Client		FALSE	Default factory setting			
Lock Outgoing Line	Enterprise Voice Client		FALSE	Default factory setting			
Reject Non-Enterprise Voice Calls	Enterprise Voice Client		FALSE	Default factory setting			
Global items							

BES IT POLICY RULES							
Policy Rule	**Policy Group**	**Setting**		**Comments**	**Security Category Code (CAT)**	**Related Check Number**	**Check If Open Finding**
		Required	**Optional**				
Allow Browser	Global		TRUE	Default factory setting. Enables BlackBerry Browser.			
Allow Phone	Global		TRUE	Default factory setting			
Auto Signature	Global		Add disclaimer message (e.g., “For government Use Only” or signature block)	If used, disclaimer message must not include “Sent from my BlackBerry handheld” or similar message.	III	WIR1210	
Location Based Services policy group (previously called BlackBerry Maps policy group)							
Disable BlackBerry Maps	Location Based Services		FALSE	Default factory setting			
Enable Enterprise Location Tracking	Location Based Services		FALSE	Default factory setting			
Enterprise Location Tracking User Prompt Message	Location Based Services		“Your location is now being tracked at the server”	Default factory setting			
Enterprise Location Tracking Interval	Location Based Services		15	Default factory setting			
MDS policy group							

BES IT POLICY RULES							
Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
		Required	Optional				
Disable activation with public MDSS	MDS	TRUE			II	WIR1230	
Disable MDS Runtime Environment	MDS		FALSE	Default factory setting			
Disable user-initiated activation with MDSS	MDS	TRUE			II	WIR1230	
Lowest security version allowed	MDS		1	Default factory setting			
Verify MDSS certificate	MDS	TRUE		Default factory setting	II	WIR1250	
Memory Cleaner policy group							
Force Memory Clean When Holstered	Memory Cleaner		TRUE				
Force Memory Clean When Idle	Memory Cleaner		TRUE				
Memory Cleaner Maximum Idle	Memory Cleaner		20				
On-Device help policy group							
On-Device Help Links	On-Device help		___	Default factory setting			
On-Device Help Group Label	On-Device help		___	Default factory setting			

BES IT POLICY RULES							
Policy Rule	**Policy Group**	**Setting**		**Comments**	**Security Category Code (CAT)**	**Related Check Number**	**Check If Open Finding**
		Required	**Optional**				
Password policy group							
Duress Notification Address	Password		NULL	Default factory setting			
Forbidden Passwords	Password	List forbidden passwords based on local security policies			III	WIR1100	
Maximum Password History	Password	3 or more			III	WIR1100	
Periodic Challenge Time	Password		60	Default factory setting. Note: When ‘Enable Long Term Timeout” is set to TRUE, this rule will be automatically set to 60.			
Set Maximum Password Attempts	Password	10 (or less)		Default factory setting	I	WIR1100	
Set Password Timeout	Password	15			II	WIR1100	
Suppress Password Echo	Password	TRUE		Default factory setting	III	WIR1100	
PIM Sync policy group							
Disable Address Wireless Sync	PIM Sync		FALSE	Default factory setting			
Disable All Wireless Sync	PIM Sync		FALSE	Default factory setting			

BES IT POLICY RULES							
Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
		Required	Optional				
Disable Calendar Wireless Sync	PIM Sync		FALSE	Default factory setting			
Disable Enterprise Activation Progress	PIM Sync		TRUE	Default factory setting			
Disable Memopad Wireless Sync	PIM Sync		FALSE	Default factory setting			
Disable Phone Call Log Wireless Sync	PIM Sync		FALSE	Default factory setting			
Disable PIN Messages Wireless Sync	PIM Sync		TRUE	Default factory setting			
Disable SMS Messages Wireless Sync	PIM Sync		TRUE	Default factory setting			
Disable Task Wireless Sync	PIM Sync		FALSE	Default factory setting			
Disable Wireless Bulk Loads	PIM Sync		FALSE	Default factory setting			
Secure Email policy group							
Canonical Certificate Domain Name	Secure Email		FALSE	Default factory setting Enter the Domain name (if this field is used)			

BES IT POLICY RULES							
Policy Rule	**Policy Group**	**Setting**		**Comments**	**Security Category Code (CAT)**	**Related Check Number**	**Check If Open Finding**
		Required	**Optional**				
Disable Certificate Address Checks	Secure Email		FALSE	Default factory setting			
Security policy group							
Allow External Connections	Security	FALSE			II	WIR1250	
Allow Internal Connections	Security		TRUE	Default factory setting			
Allow Outgoing Call When Locked	Security		FALSE	Default factory setting			
Allow Resetting of Idle Timer	Security	FALSE			II	WIR1250	
Allow Screen Shot Capture	Security		TRUE				
Allow Smart Card Password Caching	Security		FALSE	Default factory setting			
Allow Split-Pipe Connections	Security	FALSE		Default factory setting	II	WIR1250	
Allow Third Party Apps to Use Persistent Store	Security		FALSE	Use TRUE if third-party applications are allowed and persistent store required			
Allow Third Party Apps Use Serial Port	Security		FALSE	Use TRUE if third-party applications are allowed and serial port required			

BES IT POLICY RULES

Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
		Required	Optional				
Certificate Status Cache Timeout	Security	7 days or less		Default factory setting Rule removed in BES 4.1.2	III	WIR1200	
Certificate Status Maximum Expiry Time	Security	168 or less			WIR1200	III	
Content Protection Strength	Security	Stronger or Strongest			III	WIR1280	
Desktop Backup	Security		0 (All BlackBerry device databases)	Default factory setting			
Disable 3DES Transport Crypto	Security		TRUE FALSE	If using AES encryption If using 3DES encryption			
Disable Cut/ Copy/ Paste	Security		FALSE	Default factory setting			
Disable External Memory	Security		TRUE	Select FALSE if external memory cards allowed			
Disable Forwarding Between Services	Security		FALSE	Default factory setting			
Disable Geo-Tagging of Photos	Security		FALSE	Default factory setting			

BES IT POLICY RULES							
Policy Rule	**Policy Group**	**Setting**		**Comments**	**Security Category Code (CAT)**	**Related Check Number**	**Check If Open Finding**
		Required	**Optional**				
Disable Invalid Certificate Use	Security	TRUE			III	WIR1200	
Disable IP Modem	Security		FALSE	Default factory setting			
Disable Key Store Backup	Security		FALSE	Default factory setting			
Disable Key Store Low Security	Security	TRUE			III	WIR1200	
Disable Media Manager	Security		FALSE	Default factory setting			
Disable Message Normal Send	Security		FALSE	Default factory setting Set to TRUE only if S/MIME messaging is required for all email messages (forces users to send signed and/or encrypted S/MIME messages)			
Disable Peer-to-Peer Normal Send	Security	TRUE		Forces S/MIME encryption for Peer-to-Peer messages when “Allow Peer-to-Peer Message” set to “TRUE”	II	WIR1220	
Disable Persisted Plaintext	Security		FALSE	Default factory setting			
Disable Public Photo Sharing Applications	Security	TRUE			II	WIR1250	

BES IT POLICY RULES							
Policy Rule	**Policy Group**	**Setting**		**Comments**	**Security Category Code (CAT)**	**Related Check Number**	**Check If Open Finding**
		Required	**Optional**				
Disable Radio When Cradled	Security		2 - Radio disabled when the connected USB peripheral enumerates	Forces radio to turn off when BlackBerry is connected to a PC but allows radio to be on when connected to a travel charger. Set to "0" if IP modem is used.			
Disable Revoked Certificate Use	Security	TRUE			III	WIR1200	
Disable Smart Password Entry	Security		FALSE	Default factory setting			
Disable Stale Certificate Status Checks	Security		FALSE	Default factory setting			
Disable Stale Status Use	Security		FALSE	Default factory setting			
Disable Untrusted Certificate Use	Security		FALSE	Default factory setting			
Disable Unverified Certificate Use	Security		FALSE	Default factory setting			
Disable Unverified CRLs	Security	TRUE			III	WIR1200	
Disable USB Mass Storage	Security		TRUE				

BES IT POLICY RULES

Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
		Required	Optional				
Disable Weak Certificate Use	Security	TRUE			III	WIR1200	
Disallow Third Party Downloads	Security	TRUE			I	WIR1180	
External File System Encryption Level	Security	4 - Encrypt to Device Key (including multi-media directories)			III	WIR1280	
FIPS Level	Security	1 (FIPS 140-2 Level 1)		Default factory setting.	I	WIR1250	
Firewall Block Incoming Messages	Security	MMS Messages	SMS Messages		III	WIR1220	
Force Content Protection of Master Keys	Security	TRUE			I	WIR1260	
Force Include Address Book In Content Protection	Security	TRUE			III	WIR1280	
Force LED Blinking When Microphone Is On	Security	TRUE			III	WIR1250	
Force Lock When Holstered	Security		TRUE				

BES IT POLICY RULES							
Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
		Required	Optional				
Force Smart Card Two Factor Authentication	Security		FALSE	Default factory setting. Set to TRUE for CAC authentication for BlackBerry unlock.			
Force Smart Card Two Factor Challenge Response	Security		FALSE	Default factory setting			
Key Store Password Maximum Timeout	Security	60 or less (15 is the recommended setting)		Do not select 0	III	WIR1250	
Lock on Smart Card Removal	Security		FALSE	Default factory setting			
Message Classification	Security		Unclassified, Sensitive But Unclassified (SBU), Personal Identifiable Information (PII)	Specify the action (e.g. signed, encrypted or both) associated with each classification based on local or DoD policy.			
Minimal Encryption Key Store Security Level	Security	Medium Security or High Security		Default factory setting	III	WIR1250	
Minimal Signing Key Store Security Level	Security	Medium Security or High Security		Default factory setting	III	WIR1250	

BES IT POLICY RULES

Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
		Required	Optional				
Password Required for Application Download	Security	TRUE			III	WIR1250	
Required Password Pattern	Security		—	Default factory setting			
Remote Wipe Reset to Factory Defaults	Security	TRUE		If a finding, mark either WIR1090 or WIR1100	II	WIR1090 and WIR1100	
Require Secure APB Messages	Security		FALSE	Default factory setting			
Secure Wipe Delay After IT Policy Received	Security		—	Default factory setting			
Secure Wipe Delay After Lock	Security		—	Default factory setting			
Secure Wipe if Battery Low	Security		FALSE	Default factory setting			
Security Service Colors	Security		Choose message background colors				
Trusted Certificate Thumbprints	Security		—	Default factory setting			

BES IT POLICY RULES

Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
		Required	Optional				
Service Exclusivity policy group							
Allow Other Browser Services	Service Exclusivity	FALSE			II	WIR1240	
Allow Other Message Services	Service Exclusivity		FALSE				
Allow Public AIM Services	Service Exclusivity	FALSE			II	WIR1240	
Allow Public Google Talk Services	Service Exclusivity	FALSE			II	WIR1240	
Allow Public ICQ Services	Service Exclusivity	FALSE			II	WIR1240	
Allow Public IM Services	Service Exclusivity	FALSE			II	WIR1240	
Allow Public Yahoo! Messenger Services	Service Exclusivity	FALSE			II	WIR1240	
SIM Application Toolkit policy group							
Disable Network Location Query	SIM Application Toolkit		FALSE	Default factory setting			
Disable SIM Call Control	SIM Application Toolkit		FALSE	Default factory setting			

BES IT POLICY RULES							
Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
		Required	Optional				
Disable SIM Originated Calls	SIM Application Toolkit		FALSE	Default factory setting			
Smart Dialing policy group							
Enable Smart Dialing Policy	Smart Dialing		FALSE				
Set local Area Code	Smart Dialing		___	Default factory setting			
Set Local Country Code	Smart Dialing		___	Default factory setting			
Set National Number Length	Smart Dialing		___	Default factory setting			
Smart Dialing Allow Device Changes	Smart Dialing		FALSE				
S/MIME Application policy group							
Entrust Messaging Server (EMS) Email Address	S/MIME Application	___		Default factory setting	III	WIR1200	
S/MIME Allowed Content Ciphers	S/MIME Application	0 (AES-256 bit) 1 (AES-192 bit) 2 (AES-128 bit) 5 (Triple DES)			II	WIR1200	

BES IT POLICY RULES							
Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
		Required	Optional				
S/MIME Blind Copy Address	S/MIME Application		___	Default factory setting			
S/MIME Force Digital Signature	S/MIME Application		FALSE	Default factory setting. Set to TRUE based on local policy.			
S/MIME Force Encrypted Messages	S/MIME Application		FALSE	Default factory setting			
S/MIME Force Smartcard Use	S/MIME Application		TRUE	When smart card capability is available			
S/MIME Minimum Strong DH Key Length	S/MIME Application	1024		Default factory setting	III	WIR1200	
S/MIME Minimum Strong DSA Key Length	S/MIME Application	1024		Default factory setting	III	WIR1200	
S/MIME Minimum Strong ECC Key Length	S/MIME Application	163		Default factory setting	III	WIR1200	
S/MIME Minimum Strong RSA Key Length	S/MIME Application	1024		Default factory setting	III	WIR1200	
TCP policy group							
TCP APN	TCP		___	Default factory setting. Set if using TCP APN			

BES IT POLICY RULES							
Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
		Required	Optional				
TCP Password	TCP		___	Default factory setting. Set if using TCP APN			
TCP Username	TCP		___	Default factory setting. Set if using TCP APN			
TLS policy group							
TLS Device Side Only	TLS		FALSE	Default factory setting. Set to TRUE only if device-side TLS is available			
TLS Disable Invalid Connection	TLS		2 (prompt user on the BlackBerry device)	Default factory setting			
TLS Disable Untrusted Connection	TLS		2 (prompt user on the BlackBerry device)	Default factory setting			
TLS Disable Weak Ciphers	TLS		2 (prompt user on the BlackBerry device)	Default factory setting			
TLS Minimum Strong DH Key Length	TLS		1024	Default factory setting			
TLS Minimum Strong DSA Key Length	TLS		1024	Default factory setting			
TLS Minimum Strong ECC Key Length	TLS		163	Default factory setting			

BES IT POLICY RULES							
Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
		Required	Optional				
TLS Minimum Strong RSA Key Length	TLS		1024	Default factory setting			
TLS Restrict FIPS Ciphers	TLS	TRUE			III	WIR1260	
Wireless Software Upgrades policy group							
Allow Non Enterprise Upgrade	Wireless Software Upgrades	FALSE		Default factory setting Software upgrades should only come from trusted DoD source	III	WIR1250	
Disallow Device User Requested Rollback	Wireless Software Upgrades		TRUE				
Disallow device User Requested Upgrade	Wireless Software Upgrades		TRUE				
Disallow Patch Download Over International Roaming WAN	Wireless Software Upgrades	TRUE		Software upgrades should only come from trusted DoD source	III	WIR1250	
Disallow Patch Download Over Roaming WAN	Wireless Software Upgrades	TRUE		Software upgrades should only come from trusted DoD source	III	WIR1250	
Disallow Patch Download Over WAN	Wireless Software Upgrades	TRUE		Software upgrades should only come from trusted DoD source	III	WIR1250	
Disallow Patch Download Over WiFi	Wireless Software Upgrades	TRUE		Software upgrades should only come from trusted DoD source	III	WIR1250	

BES IT POLICY RULES							
Policy Rule	Policy Group	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
		Required	Optional				
WTLS (Application) policy group							
WTLS Disable Invalid Connection	WTLS		2 (prompt user on the BlackBerry device)	Default factory setting			
WTLS Disable Untrusted connection	WTLS		2 (prompt user on the BlackBerry device)	Default factory setting			
WTLS Disable Weak Ciphers	WTLS		2 (prompt user on the BlackBerry device)	Default factory setting			
WTLS Minimum Strong DH Key Length	WTLS		1024	Default factory setting			
WTLS Minimum Strong ECC Key Length	WTLS		163	Default factory setting			
WTLS Minimum Strong RSA Key Length	WTLS		1024	Default factory setting			
WTLS Restrict FIPS Ciphers	WTLS	TRUE		Default factory setting	III	WIR1260	

Table C.1. BES IT Policy Rules

This page is intentionally blank.

APPENDIX D. HANDHELD SOFTWARE CONFIGURATION SETTINGS

BLACKBERRY HANDHELD SOFTWARE CONFIGURATION SETTINGS						
Rule	**Setting Required**	**Optional**	**Comments**	**Security Category Code (CAT)**	**Related Check Number**	**Check If Open Finding**
Options/Bluetooth/Paired Devices list/select each paired device/click Device Properties						
Device Name	Leave default value			III	WIR1250	
Trusted	Ask			III	WIR1250	
Encryption	Enabled		May not be able to configure on device if corresponding BES IT Policy rule is configured	III	WIR1250	
“Don’t ask this again” checkbox	Do Not Check		Located on the connection alert dialog box	III	WIR1250	
Options/Bluetooth/Options menu item						
Device Name	Select name that does not identify user, organization, location, or device in any way			III	WIR1250	
Discoverable	No		May not be able to configure on device if corresponding BES IT Policy rule is configured	II	WIR1140	

BLACKBERRY HANDHELD SOFTWARE CONFIGURATION SETTINGS						
Rule	**Setting Required**	**Optional**	**Comments**	**Security Category Code (CAT)**	**Related Check Number**	**Check If Open Finding**
Allow Outgoing Calls	If Unlocked		May not be able to configure on device if corresponding BES IT Policy rule is configured	III	WIR1250	
Address Book Transfer	Disabled		May not be able to configure on device if corresponding BES IT Policy rule is configured	III	WIR1250	
Options/Security Options/Smart Card						
Lock on Card Removal		Disabled	May not be able to configure on device if corresponding BES IT Policy rule is configured			
PIN Caching		Disabled	May not be able to configure on device if corresponding BES IT Policy rule is configured			
Options/Security Options/Smart Card/Registered Reader Drivers/BlackBerry/Driver Settings						
Reader LED – Low Battery	Enabled			III	WIR1150	
Reader LED – Pairing	Enabled			III	WIR1150	
Reader LED – Traffic	Enabled			III	WIR1150	

BLACKBERRY HANDHELD SOFTWARE CONFIGURATION SETTINGS						
Rule	**Setting Required**	**Optional**	**Comments**	**Security Category Code (CAT)**	**Related Check Number**	**Check If Open Finding**
Reader Setting – Connection Heartbeat Period		None	May not be able to configure on device if corresponding BES IT Policy rule is configured			
Reader Setting – Power Off Timeout		None				
Reader Setting – Power saving Mode		Partial				
Reader setting – Bluetooth Range	2 or less		May not be able to configure on device if corresponding BES IT Policy rule is configured	III	WIR1150	
Erase Key After – Disconnected Timeout		None	May not be able to configure on device if corresponding BES IT Policy rule is configured			
Erase Key After – Long Term Timeout		None	May not be able to configure on device if corresponding BES IT Policy rule is configured			
Erase Key After – Inactivity Timeout		None	May not be able to configure on device if corresponding BES IT Policy rule is configured			

BLACKBERRY HANDHELD SOFTWARE CONFIGURATION SETTINGS						
Rule	**Setting Required**	**Optional**	**Comments**	**Security Category Code (CAT)**	**Related Check Number**	**Check If Open Finding**
Erase Key After – Card Not Present timeout		None	May not be able to configure on device if corresponding BES IT Policy rule is configured			
Erase Key After – Number of Transactions		None	May not be able to configure on device if corresponding BES IT Policy rule is configured			
Options/Owner						

BLACKBERRY HANDHELD SOFTWARE CONFIGURATION SETTINGS						
Rule	**Setting Required**	**Optional**	**Comments**	**Security Category Code (CAT)**	**Related Check Number**	**Check If Open Finding**
Name	Leave blank or follow guidance in comment		May not be able to configure on device if corresponding BES IT Policy rule is configured DoD BlackBerry sites should consider using the following message: "If this BlackBerry is found, please call the following phone number xxx-xxx-xxxx." When called, the phone number should not identify itself as a DoD organization.	III	WIR1250	

BLACKBERRY HANDHELD SOFTWARE CONFIGURATION SETTINGS						
Rule	**Setting Required**	**Optional**	**Comments**	**Security Category Code (CAT)**	**Related Check Number**	**Check If Open Finding**
Information	Leave blank or follow guidance in comment		May not be able to configure on device if corresponding BES IT Policy rule is configured DoD BlackBerry sites should consider using the following message: "If this BlackBerry is found, please call the following phone number xxx-xxx-xxxx." When called, the phone number should not identify itself as a DoD organization.	III	WIR1250	

Table D.1. BlackBerry Handheld Software 4.1 Configuration Settings

This page is intentionally blank.

APPENDIX E. CAC DIGITAL CERTIFICATE PROVISIONING

1. Initial Provisioning of BlackBerry for S/MIME

Complete the following steps for setting up a BlackBerry with S/MIME support:

- Load BlackBerry Handheld and carrier software on BlackBerry.
- Load S/MIME software on BlackBerry.
- Load Smart Card Reader drivers on BlackBerry.
- Load Smart card reader drivers on Bluetooth SCR.
- Load user digital certificates on BlackBerry.
- Load DoD Root certificates on BlackBerry (to get the latest root certificates, use the BlackBerry browser and connect to www.dodpke.com/jad and download Root Certificate file.)

Download the following documents from the DoD PKE web portal for additional information:

BlackBerry QRC Importing Smart Card Certs.pdf
BlackBerry SMIME and SCR for CAC Setup.pdf

These documents are located at https://gesportal.dod.mil/sites/dodpke/ , select the "Knowledge Base Library" link, select the "Wireless" folder, then the "BlackBerry" folder.

2. Loading New CAC Public Certificates on a BlackBerry

Follow the following procedure for loading certificates from a new CAC on a previously provisioned BlackBerry:

- Load new certificates by following the procedures found in BlackBerry QRC Importing Smart Card Certs.pdf (see #1 above).
- Remove old certs from BlackBerry as follows:
  - Connect BlackBerry to computer where BlackBerry Desktop Manager is installed with USB cable.
  - Launch the BlackBerry Desktop Manager.
  - Click on "Certificate Sync."
  - Under the "Personal Certificates" tab, uncheck all old certificates.
  - Click "Synchronize."

For additional information or assistance on BlackBerry PKI issues, contact the DoD PKE office at pke_support@disa.mil or visit their web site at https://gesportal.dod.mil/sites/dodpke/.

This page is intentionally blank.

APPENDIX F. VMS PROCEDURES

The following information applies only to teams and sites that use VMS to enter and track DoD assets. When conducting a BlackBerry SRR, the Team Lead and the assigned Reviewer identify security deficiencies, provide data from which to predict the effectiveness of proposed or implemented security measures associated with the BlackBerry system and operating environment. Security Readiness Review (SRR) of a DoD BlackBerry system requires that the results of the SRR be tracked using the VMS database.

Both the Reviewer and the SA will create, maintain, and track assets in VMS. The reviewer will use the Asset and Finding Maintenance screen to perform these functions. The SA will use the By Location navigation chain to perform the same function. When Reviewers access the Asset and Finding Maintenance screen, the Navigation pane displays a white Visits folder. Expand this Visits folder to display its subfolders. Each subfolder represents an individual visit in VMS that is assigned for review. Click (+) to expand the visit and display the location summaries for the visit. Within the location, BlackBerry assets are tracked using the Computing asset type.

Use the following matrix to select the appropriate asset type for each BlackBerry asset. The reviewer or SA must enter the entire asset posture including non-wireless related applications and services installed on the BES.

VMS Asset Matrix		
Wireless Technology	**VMS Asset Type**	**ASSET POSTURE**
BlackBerry Enterprise Server ***NOTE:*** Only configure asset for applications installed on the **same** server as the BES application. There are no checks for LDAP	Computing	**Operating System –**> Windows. Expand and select version then service pack installed. **Application –**BlackBerry Enterprise Server **Application –**>Antivirus. Expand and select version. **Application –** Expand and select other applications installed on same server to capture the entire asset posture of the server (e.g., SQL, Exchange, Browsers, Office Automation, etc). **Role –** Member Server
BlackBerry Client Devices	Computing	***NOTE:*** Do not mark as a workstation ***NOTE:*** Do not enter IP or MAC address **Network** –> Data Network -> Wireless -> BlackBerry Client

Table E-1. VMS Asset Matrix

This page is intentionally blank.

APPENDIX G. BLACKBERRY CONFIGURATION FOR GROUP EMAIL ACCOUNTS

Procedures for Setting up and Using a "Team" BlackBerry

Introduction

When a BlackBerry has been set up for a group email account and will be shared by a group or "team" (e.g. help desk team) the BlackBerry must be configured and operated consistent with DoD BlackBerry security requirements. This paper describes required procedures.

References

1. BlackBerry QRG Importing Software Certs.pdf, found on the DoD PKE web site at https://gesportal.dod.mil/sites/dodpke/, select the "Knowledge Base Library" link, select the "Wireless" folder, then the "BlackBerry" folder.
2. BlackBerry QRG Importing Smart card Certs.pdf, found on the DoD PKE web site at https://gesportal.dod.mil/sites/dodpke/, select the "Knowledge Base Library" link, select the "Wireless" folder, then the "BlackBerry" folder.

Step 1 – Install Group Email Account Shared Email Encryption Key on BlackBerry

a. Have Team Lead follow local procedures to request a software certificate from the local RA. Request group/role attributes for the group email account.

b. Get the private email encryption key and save on floppy diskette or thumb drive. The team lead must select a master password to protect the key and the password should only be known to the team lead.

c. Install private email encryption key for group email account on the PC used as the Desktop Manager for the Team BlackBerry. (See Reference 1, Steps 5-16)

   Once the two new .cer files have been created, publish the group email account certificates to the GAL using local procedures.

d. Mark key as exportable. (See Reference 1, Step 9)

e. Export key to the BlackBerry. (See Reference 1, Steps 17-19)

f. Re-install private email encryption key to the desktop a second time (see paragraph c above) and mark as non-exportable. (See Reference 1, follow procedure described at the end of page 6)

g. If BlackBerry Desktop Manager and private group email encryption key is installed on every team member's PC then there will be less disruption when a member of the team departs the group. This minimizes the security risk when a member of the group leaves, thus requiring the group email certificate keystore password to be changed. Each team member than selects their own certificate keystore password to protect the certificates on their PC.

Step 2 - Install Team Member certificates on BlackBerry
Load the digital certificates of each team member on the BlackBerry. (See Reference 2)

STEP 3 – Incorporate BlackBerry Team Procedures in Site BlackBerry SOP/CONOPS
The following procedures must be included in the site BlackBerry SOP or CONOPS:

a. Each "team" member is required to logon to the BlackBerry with their CAC.

- Configure the BlackBerry or BES to require CAC authentication for device unlock. Do one of the following:
    - Put Team BlackBerry in a separate IT Policy group on the BES and enable "**Force Smart Card Two Factor Authentication**."
    Or
    - On team BlackBerry, Enable "**User Authentication**" (e.g. CAC authentication) as follows[2]: **Options**>**Security Options**>**General Settings**>click on **User Authentication**>select **Change Option**>change option to **Enabled**>click **User Authentication**>select **Save**>when prompted, enter BlackBerry password under **Enter Handheld Password** (or **Enter Password**) and enter CAC PIN of current team member using BlackBerry under **Enter Authenticator Password.**

  Note: Both the BlackBerry password and the CAC PIN need to be entered when unlocking the BlackBerry.

- Procedure for changing Team BlackBerry user:
    - The **User Authentication Password** must be changed to the new user's CAC PIN as follows:
    - Current user unlocks the BlackBerry
    - Current user selects **Options**>**Security Options**>**General Settings**>click on **User Authentication**>select **Change Option**>**Change Password**> when prompted, enter BlackBerry password under **Enter Handheld Password** and enter CAC PIN of current team member using BlackBerry under **Enter Authenticator Password**
    - When **New Password** prompt is on screen, hand BlackBerry to new user.
    - New user enters CAC PIN and then reenters PIN to verify new Authentication Password.

b. Each "team" member is to be trained on how to sign and encrypt email messages on the BlackBerry.

[2] This procedure may vary slightly, depending on the BlackBerry model and version of Handheld Software installed.

c. BlackBerry team members are prohibited from storing personal or individually sensitive information on the team BlackBerry.

d. A "Master Station Log" will be used to document who currently has possession of the team BlackBerry and when the BlackBerry was passed from one team member to another. Procedures for maintaining and inspecting the log will also be included in the site BlackBerry SOP or CONOPS.

e. Completion of BlackBerry user training will be documented.

This page is intentionally blank.